Die Rolle der Internet Service Provider im deutschen und US-amerikanischen Recht

Verantwortlichkeit und Privilegierung für Urheberrechtsverletzungen im Internet

Inaugural-Dissertation
zur
Erlangung der Doktorwürde
einer Hohen Rechtswissenschaftlichen Fakultät
der Universität zu Köln

vorgelegt von

Rilana Wenske

aus: Dernbach

Referent:	Professor Dr. Karl-Nikolaus Peifer
Korreferent:	Juniorprofessorin Dr. Louisa Specht
Tag der mündlichen Prüfung:	15.12.2016

Inhaltsverzeichnis

ABKÜRZUNGSVERZEICHNIS XVIII
LITERATURVERZEICHNIS XXV
SONSTIGE QUELLEN XLVII
A. EINFÜHRUNG 1
I. DIE HAFTUNG DER INTERNET SERVICE PROVIDER 1
II. PROBLEMSTELLUNG UND ARBEITSHYPOTHESE 3
III. METHODIK DER UNTERSUCHUNG 6
IV. STAND DER FORSCHUNG 7
V. GANG DER UNTERSUCHUNG 10
B. TECHNISCHE UND BEGRIFFLICHE GRUNDLAGEN 11
I. DAS INTERNET 12
1. World Wide Web 13
2. File Transfer Protocol 14
3. Proxy-Server 14
4. Usenet 14
5. Peer-to-Peer 15
6. Hyperlinks und Deep-Links 16
7. Framing/In-line Linking 16
8. Netzsperren 17
a) DNS-Sperre 17
b) IP-Sperre 17
c) URL-Sperre 18
II. TELEMEDIEN 18
1. Positives Abgrenzungsmerkmal 18
a) Dienst 19
b) Elektronisch 19
c) Information und Kommunikation 19
2. Negative Abgrenzungsmerkmale 19
a) Telekommunikationsdienste 20
b) Telekommunikationsgestützte Dienste 21
c) Rundfunk 21
III. INTERNET SERVICE PROVIDER 22
1. Content-Provider 23

2. Host-Provider 23
3. Cache-Provider 24
4. Access-Provider/Network-Provider 24
C. VERANTWORTLICHKEIT UND PRIVILEGIEN DER ISP IN DEUTSCHLAND 25
I. HAFTUNGSPRIVILEGIEN NACH §§ 7 FF. TMG 25
1. Gesetzgebungsgeschichte 26
a) IuKDG 26
b) EGG 27
c) EIGVG 27
2. Anwendungsbereich 28
3. Adressaten 28
4. Dogmatische Einordnung 29
a) Einstufiges Modell 29
aa) Schuldebene 29
bb) Rechtswidrigkeitsebene 30
cc) Tatbestandsebene 30
b) Zweistufiges Modell 31
aa) Nachfilter 31
bb) Vorfilter 32
5. Einzelne Privilegierungstatbestände 34
a) Allgemeine Grundsätze 34
aa) Keine allgemeine Überwachungs- und Nachforschungspflicht 34
(1) EuGH-Urteile: SABAM/Scarlet und SABAM/Netlog 35
(2) Bewertung der EuGH-Urteile 36
bb) Verpflichtung zur Sperrung/Entfernung 38
b) Host-Provider, § 10 TMG 39
aa) Personeller Anwendungsbereich 40
bb) Fremde Informationen i.S.d. § 10 TMG 40
(1) Abgrenzung zu eigenen Informationen 42
(2) Zu eigen gemachte Informationen 42
(a) Rechtsprechung des BGH 43
(b) Vereinbarkeit mit der ECRL 44
(c) Rechtsprechung des EuGH – „aktive Rolle“ 46

(d) Ergebnis 49
cc) Fehlende Kenntnis 49
(1) Kenntnis der rechtswidrigen Handlung oder der Information 50
(2) Positive Kenntnis 52
(3) Offensichtlichkeit/Umstandskenntnis 53
(4) Bewusstes Wegschauen 54
(5) Vermutete Kenntnis - Gesetzentwurf zur Änderung des TMG 55
(a) Wortlaut der gesetzlichen Vermutung der Kenntnis 55
(b) Begründung der gesetzlichen Vermutung der Kenntnis 56
(c) Beschlussempfehlung des Deutschen Bundestags und Bewertung der gesetzlichen Vermutung der Kenntnis 56
dd) Wissenszurechnung 58
ee) Unverzügliches Tätigwerden nach Kenntniserlangung 59
ff) Kein Unterordnungs- bzw. Beaufsichtigungsverhältnis 61
gg) Anwendbarkeit auf Unterlassungsansprüche 62
(1) Frühe Rechtsprechung des BGH 62
(a) Wortlaut 63
(b) § 8 Abs. 2 TDG a.F./Art. 14 Abs. 3 ECRL 63
(c) Schadensersatzanspruch v. Unterlassungsanspruch 63
(d) § 5 Abs. 4 TDG a.F. 64
(e) Vorbeugende Unterlassungsansprüche 64
(f) Zwischenergebnis 64
(2) Bewertung der früheren Rechtsprechung des BGH 65
(a) Wortlaut-Argument 66
(b) § 8 Abs. 2 TDG n.F./Art. 14 Abs. 3 ECRL 66
(c) Schadensersatzanspruch v. Unterlassungsanspruch 68
(d) § 5 Abs. 4 TDG a.F. 69
(e) Vorbeugende Unterlassungsansprüche 69
(f) Zwischenergebnis 70
(3) EuGH-Urteil L'Oréal 71
(4) Bewertung L'Oréal-Urteil 73
(5) Weiterentwicklung der Rechtsprechung des BGH 76
(6) Bewertung der Weiterentwicklung der Rechtsprechung des BGH 77
(7) Ergebnis 79

hh) Fazit 81
c) Cache-Provider 81
aa) Anwendungsbereich 82
bb) Keine Veränderung der Information 84
cc) Beachten von Zugangsbedingungen 85
dd) Beachtung von Industriestandards für die Aktualisierung 85
ee) Keine Beeinträchtigung der Sammlung von Daten 86
ff) Unverzügliche Entfernung/Sperrung 87
gg) Keine Zusammenarbeit mit dem Nutzer 88
hh) Anwendbarkeit auf Unterlassungsansprüche 89
ii) Fazit 90
d) Access Provider 90
aa) Anwendungsbereich 90
bb) Keine Veranlassung der Übermittlung 91
cc) Keine Auswahl des Adressaten 92
dd) Keine Auswahl oder Veränderung der übermittelten Informationen 92
ee) Keine Zusammenarbeit mit dem Nutzer 92
ff) Gleichstellung automatischer kurzzeitiger Zwischenspeicherung 93
(1) Automatische kurzzeitige Zwischenspeicherung 94
(2) Nur zur Durchführung der Übermittlung 94
(3) Keine längere Speicherung als üblicherweise erforderlich 94
gg) Anwendbarkeit auf WLAN-Betreiber 95
(1) BGH Rechtsprechung zu privaten WLAN-Anschluss 96
(2) Bewertung der Rechtsprechung zu privaten WLAN-Anschluss 97
(3) Abweichende unterinstanzliche Rechtsprechung zu privatem WLAN-Anschluss 98
(4) Rechtsprechung zu gewerblichen WLAN-Anschlüssen 98
(5) Vorabentscheidungsersuchen des LG München I 100
(6) Bewertung Rechtsprechung zu gewerblichen WLAN-Anschlüssen 103
hh) Anwendbarkeit der Haftungsprivilegien auf Unterlassungsansprüche 105
(1) „Goldesel“- und 3dl.am-Entscheidung des BGH 106
(2) Bewertung „Goldesel“- und „3dl.am“-Entscheidung des BGH 107
(3) Vorabentscheidungsersuchen des LG München I 108

(4) Anwendbarkeit auf Unterlassungsansprüche nach dem neuen WLAN-Gesetz 110
(5) Ergebnis 111
ii) Fazit 112
e) Sonstige ISP 112
aa) Anbieter von Hyperlinks 113
bb) Suchmaschinen-Anbieter 115
(1) Anzeigen von Ergebnislisten auf Suchanfrage 115
(2) Anzeigen von Vorschaubildern in Ergebnislisten 116
(3) Autocomplete-Funktion 117
(4) Fazit 119
6. Ergebnis 119
II. VERANTWORTLICHKEIT FÜR URHEBERRECHTSVERLETZUNGEN NACH DEN ALLGEMEINEN GESETZEN 120
1. Zivilrechtliche Verantwortlichkeit des Host-Providers 120
a) Täter/Teilnehmer 120
aa) Täter 120
bb) Teilnehmer 121
(1) Anstifter 122
(2) Gehilfe 123
(a) Urteil des OLG Hamburg 123
(b) Bewertung 124
(c) Rechtsprechung des BGH 126
(d) Zwischenergebnis 127
cc) Rechtsfolgen 127
(1) Beseitigungs- und Unterlassungsanspruch, § 97 Abs. 1 UrhG 127
(2) Schadensersatzanspruch, § 97 Abs. 2 UrhG 128
b) Störer 128
aa) Spannungsverhältnis § 10 TMG und Störerhaftung 130
bb) Zumutbare Prüfpflichten nach Kenntnis 131
cc) Umfang der Prüfpflicht- Kerngleichheit 133
dd) Bewertung Prüfpflichten 134
ee) Zwischenergebnis 138
ff) Rechtsfolgen 138

(1) Beseitigungs- und Unterlassungsanspruch, § 97 Abs. 1 UrhG 139
(2) Schadensersatzanspruch, § 97 Abs. 2 UrhG 140
c) Ergebnis 142
2. Strafrechtliche Verantwortlichkeit des Host-Providers 143
a) Unerlaubte Verwertung urheberrechtlich geschützter Werke, § 106 UrhG 143
aa) In anderen als den gesetzlich zugelassenen Fällen 143
bb) Vervielfältigung, Verbreitung oder öffentliche Wiedergabe 144
cc) Vorsatz 144
dd) Keine Einwilligung 144
b) Gewerbsmäßige unerlaubte Handlung, § 108a UrhG 145
c) Ergebnis 145
3. Zivilrechtliche Verantwortlichkeit des Cache-Providers 146
a) Täter/Teilnehmer 146
b) Störer 147
aa) Spannungsverhältnis § 9 TMG und Störerhaftung 148
bb) Zumutbare Prüfungspflichten nach Kenntnis - bisherige Rechtsprechung 148
cc) Bewertung der bisherigen Rechtsprechung 150
dd) Zumutbare Prüfpflichten nach Kenntnis - „post-Stiftparfum“ 151
ee) Bewertung 152
ff) Rechtsfolgen 153
(1) Beseitigungs- und Unterlassungsanspruch, § 97 Abs. 1 UrhG 153
(2) Schadensersatzanspruch, § 97 Abs. 2 UrhG 154
c) Ergebnis 155
4. Strafrechtliche Verantwortlichkeit des Cache-Providers 156
5. Zivilrechtliche Verantwortlichkeit des Access-Provider 156
a) Täter/Teilnehmer 156
b) Störer 157
aa) EuGH-Urteil zu Sperrverfügungen 157
bb) Bewertung EuGH-Rechtsprechung 158
cc) BGH-Entscheidung 159
dd) Bewertung der BGH-Rechtsprechung 163
(1) Störerhaftung 163
(2) Grundrechtsabwägung 169
(3) Effektivität der Sperrmaßnahmen 170

(4) Eingriff in das Fernmeldegeheimnis, Achtung der Kommunikation 170
(5) Fehlende spezialgesetzliche Grundlage 172
(6) Eingriff in den Schutz personenbezogener Daten - Recht auf informationelle Selbstbestimmung 173
(7) Vorhergehende Inanspruchnahme vorrangig Beteiligter 175
(8) Ergebnis 175
c) Zivilrechtliche Verantwortlichkeit des WLAN-Anbieters 176
aa) Rechtsfolgen 177
(1) Beseitigungs- und Unterlassungsanspruch, § 97 Abs. 1 UrhG 177
(2) Schadensersatzanspruch, § 97 Abs. 2 UrhG 178
d) Ergebnis 178
6. Strafrechtliche Verantwortlichkeit des Access-Providers 181
7. Zivilrechtliche Verantwortlichkeit des Linksetzenden und Suchmaschinenanbieters 181
a) Hyperlinks und Deeplinks 181
aa) Paperboy-Entscheidung des BGH 181
bb) Session-ID-Entscheidung des BGH 183
cc) Svensson-Entscheidung des EuGH 183
dd) Zwischenergebnis 184
ee) Schöner Wetten-Entscheidung des BGH 185
ff) ueber18.de-Entscheidung des BGH 186
gg) Haftung für Hyperlink-Urteil des BGH 187
hh) Zwischenergebnis 188
b) Framing 189
aa) Die Realität-Entscheidung des BGH 190
bb) BestWater-Entscheidung des EuGH 191
cc) Zwischenergebnis 191
dd) Die Realität II-Entscheidung des BGH 192
ee) Zwischenergebnis 193
c) Suchmaschinen-Anbieter 194
aa) Anzeigen von Ergebnislisten auf Suchanfrage 194
bb) Anzeigen von Vorschaubildern in Ergebnislisten 196
cc) Zwischenergebnis 197
dd) Rechtsfolgen 198
(1) Beseitigungs- und Unterlassungsanspruch, § 97 Abs. 1 UrhG 198

(2) Schadensersatzanspruch, § 97 Abs. 2 UrhG 198
d) Ergebnis 199
8. Strafrechtliche Verantwortlichkeit des Linksetzenden und Suchmaschinenanbieters 201
a) Kino.to-Urteil des LG Leipzig 201
b) Bewertung des Kino.to-Urteils des LG Leipzig 202
c) Ergebnis 204
III. Sonstige Ansprüche des Urheberrechtsinhabers gegen den ISP 204
1. Offensichtliche Rechtsverletzung oder anhängiges Verfahren 205
2. Gewerbliches Ausmaß 206
3. Gegenstand des Auskunftsverlangens 207
a) Bestands- und Nutzungsdaten 208
b) Verkehrsdaten 210
c) Abgrenzung TMG und TKG 212
IV. Haftung des ISP gegenüber dem Nutzer 213
1. Vertragliche Ansprüche des Nutzers 214
a) Vertragliche Ansprüche gegenüber dem Host-Provider 214
aa) Vertragsrechtliche Einordnung des Hosting-Vertrags 214
bb) Ansprüche aus dem Hosting-Vertrag 215
b) Vertragliche Ansprüche gegenüber dem Access-Provider 216
aa) Vertragliche Einordnung des Access-Provider-Vertrags 216
bb) Ansprüche aus dem Access-Provider-Vertrag 216
c) Ausschluss vertraglicher Ansprüche durch AGB 217
2. Gesetzliche Ansprüche des Nutzers 218
a) Gesetzliche Ansprüche gegenüber dem Host-Provider 218
aa) Eigentum 218
bb) Sonstiges Recht 219
(1) Schutz von Daten – Recht auf Integrität und Vertraulichkeit informationstechnischer Systeme 219
(2) Eingerichteter und ausgeübter Gewerbebetrieb 220
cc) Rechtswidrigkeit 221
dd) Schuldhafte Verletzung 223
b) Gesetzliche Ansprüche gegenüber dem Access-Provider 223
aa) Haftung wegen Sperrung des Zugangs zu Informationen 224
bb) Haftung wegen Sperrung eigener Inhalte durch Access-Provider 225

(1) Eingerichteter und ausgeübter Gewerbebetrieb 226
(2) Recht auf Integrität und Vertraulichkeit informationstechnischer Systeme 226
(3) Urheberrecht 227
(4) Rechtswidrigkeit 227
(5) Verschulden 228
c) Gesetzliche Ansprüche gegen den Cache-Provider 228
d) Gesetzliche Ansprüche gegen den Suchmaschinenanbieter 228
3. Ergebnis 229
V. SELBSTREGULATORISCHE MAßNAHMEN DER ISP 229
VI. ZUSAMMENFASSUNG 232
D. VERANTWORTLICHKEIT UND PRIVILEGIEN DER ISP IN DEN USA 232
I. EINFÜHRUNG IN DAS U.S.-AMERIKANISCHE RECHT 232
1. Rechtsquellen 233
a) Richterrecht - Case Law 233
b) Kodifiziertes Recht - Statutes 233
aa) Gesetzgebung 234
bb) Gesetzesauslegung 235
2. Gerichtsbarkeit 235
3. U.S.-amerikanisches Urheberrecht 236
II. ALLGEMEINE HAFTUNGSREGELN 236
1. Direct und indirect infringer 236
a) Direct Infringer 237
b) Indirect Infringer 238
aa) Contributory Infringement 238
bb) Vicarious Infringement 240
cc) Inducement Liability 241
c) Rechtsfolgen 243
aa) Unterlassung - Injunctions 243
bb) Schadensersatz – Damages 243
III. HAFTUNGSPRIVILEGIEN NACH § 512 DMCA 244
1. Gesetzgebungsgeschichte 245
2. Anwendungsbereich 247
3. Adressaten 248

4. Dogmatische Einordnung 248
5. Einzelne Privilegierungstatbestände 250
a) Allgemeine Voraussetzungen für eine Privilegierung 250
aa) Service Provider, § 512 (k) (1) DMCA 251
(1) Service Provider gem.§ 512 (a) DMCA - Access-Provider 251
(2) Service Provider gem. § 512 (b) – (d) DMCA 253
bb) *Repeat Infringer Policy* § 512 (i) (1) (A) DMCA 253
(1) Policy zum Ausschluss von Wiederholungstätern 254
(2) Angemessene Umsetzung 259
(3) Benachrichtigung der Abonnenten/Kontoinhaber 261
(4) Anwendbarkeit auf ISP ohne Abonnenten/Kontoinhaber 261
cc) Standard Technical Measures 263
dd) Protection of Privacy 264
b) Host-Provider 266
aa) Speicherung auf Anweisung des Nutzers 266
bb) Material auf dem System/Netzwerk des Host-Providers 269
cc) Kenntnis und unverzügliches Tätigwerden 269
(1) Keine tatsächliche Kenntnis – No actual knowledge 270
(2) No awareness - Keine Red Flag knowledge 272
(a) Kritik 275
(b) Bewertung 278
(c) Ergebnis 280
(3) Sonderfall: Willful Blindness 282
(a) Actual knowledge/Awareness durch Willful Blindness 283
(b) Kritik 284
(c) Bewertung 285
(4) Keine zügige Entfernung bzw. Sperrung des Materials 286
dd) Kein finanzieller Vorteil und keine Kontrolle 287
(1) Direkter finanzieller Vorteil 288
(2) Bewertung 289
(3) Kein Recht und keine Möglichkeit zur Kontrolle 292
(4) Bewertung 295
ee) Notice and Takedown-Verfahren 296
(1) Benannter Bevollmächtigter - Designated agent 299

(2) Notification 300
(a) Unterschrifterfordernis 302
(b) Bezeichnung des urheberrechtlich geschützten Werkes 303
(c) Bezeichnung des urheberrechtsverletzenden Materials 303
(d) Angabe von Kontaktdaten 306
(e) Erklärung nach gutem Glauben 306
(f) Korrektheit der Angaben 309
(3) Folgen einer unvollständigen Notification 309
(4) Benachrichtigung des behaupteten Rechtsverletzers 310
(5) Abweichungen von dem gesetzlich vorgegebenen System 310
ff) Fazit 311
c) Cache-Provider 313
aa) Caching im Sinne des § 512 (b) 314
bb) Weitere Voraussetzungen der Privilegierung 314
(1) Keine Veränderung des Materials 314
(2) Beachtung von Vorgaben bzgl. der Aktualisierung 315
(3) Keine Beeinträchtigung des Erhalts bestimmter Informationen 316
(4) Beachtung von Zugangsbedingungen 317
(5) Unverzügliche Entfernung/Sperrung 317
cc) Einschlägige Rechtsprechung 318
dd) Fazit 319
d) Access-Provider 320
aa) Voraussetzungen 321
(1) Vom Nutzer initiierte Übertragung 321
(2) Keine Auswahl des Materials 321
(3) Keine Auswahl der Empfänger 322
(4) Keine dauerhafte Kopie 322
(5) Keine Veränderung des Inhalts 323
bb) Anwendbarkeit auf WLAN-Betreiber 323
cc) Fazit 325
e) Information Location Tools 325
aa) Keine tatsächliche Kenntnis – No actual knowledge 326
bb) No awareness – Keine red flag knowledge 327
cc) Entfernung bzw. Sperrung des Materials 329

dd) Finanzieller Vorteil und Kontrolle 329
ee) Notice and Takedown-Verfahren 329
ff) Allgemeine und spezialisierte Suchmaschinen 330
gg) Fazit 332
f) Counter notification 333
aa) Voraussetzungen der counter notification 333
bb) Anwendungsbereich 335
g) Put back procedure 336
h) Haftung gegenüber dem Nutzer 337
i) Haftung für falsche Darstellung - Misrepresentations 338
aa) Dancing Baby-Entscheidung des Ninth Circuit 339
bb) Bewertung 343
cc) Fazit 343
j) Anordnung zur Identifizierung des Rechtsverletzers 345
6. Umfang der Privilegierung 349
a) Host-, Cache-Provider und Information Location Tools 351
aa) Entfernung/Sperrung 351
bb) Ausschluss des Rechtsverletzers 351
cc) Sonstige notwendige Anordnungen 351
b) Access-Provider 351
aa) Ausschluss des Rechtsverletzers 352
bb) Sperrverfügung 352
c) Fazit 353
7. Ergebnis 354
8. Verbesserungsvorschläge 358
a) Eidesstattliche Versicherung des guten Glaubens 358
b) Verzögerung des Takedown 358
c) Unverzügliche Wiederherstellung nach counter notification 359
d) Verschärfung der Rechtsbehelfe gegen unberechtigte notifications 360
e) Information zur counter notification 361
f) Einrichtung eines zentralen Registers 361
IV. VERANTWORTLICHKEIT DER ISP NACH DEN ALLGEMEINEN GESETZEN 362
1. Zivilrechtliche Verantwortlichkeit des Host-Providers 362
a) Direct infringer 362

b) Indirect infringer 364
aa) Contributory liability 364
bb) Vicarious liability 365
cc) Inducement liability 365
2. Strafrechtliche Verantwortlichkeit des Host-Providers 366
3. Zivilrechtliche Verantwortlichkeit des Cache-Providers 369
a) Direct Infringer 370
b) Indirect Infringer 371
aa) Contributory Infringement 371
bb) Vicarious infringement 372
cc) Inducement liability 372
4. Strafrechtliche Haftung des Cache-Providers 373
5. Zivilrechtliche Verantwortlichkeit des Access-Providers 373
a) Direct infringer 374
b) Indirect infringer 375
aa) Contributory liability 375
bb) Vicarious liability 377
cc) Inducement liability 377
c) Zivilrechtliche Verantwortlichkeit des WLAN-Anbieters 378
6. Strafrechtliche Verantwortlichkeit des Access-Providers 380
7. Zivilrechtliche Verantwortlichkeit der Information Location Tools 380
a) Direct infringer 380
b) Indirect infringer 381
8. Strafrechtliche Verantwortlichkeit der Information Location Tools 383
V. Selbstregulatorische Maßnahmen der ISP 386
1. User Generated Content Principles 386
2. Copyright Alert System 387
a) Funktionsweise des Copyright Alert System 388
b) Kritik 389
c) Fazit 391
VI. Zusammenfassung 392
E. RECHTSVERGLEICH UND ANALYSE 395
I. Allgemein 396
1. Umfang der Haftungsprivilegien 396

2. Ausschluss Rechtsverletzer ... 398
3. Auskunftsverpflichtung ... 399
4. Verantwortlichkeit ggü. Nutzer ... 401
II. HOST-PROVIDER ... 402
1. Aktiver ISP/right and ability to control ... 402
2. Informationen Dritter ... 404
3. Kenntnis ... 405
4. Förderung von Rechtsverletzungen ... 408
5. Take-Down v. Stay-Down ... 410
a) Notice v. Kenntnis ... 411
b) Benachrichtigung des Nutzers ... 412
c) Verteidigungsmöglichkeiten des betroffenen Nutzers ... 413
d) Put back-Verfahren ... 414
e) Haftung gegenüber dem Nutzer ... 415
f) Haftung für falsche Darstellung ... 416
aa) Ansprüche Host-Provider gegen Urheberrechtsinhaber ... 417
bb) Ansprüche vermeintlicher Rechtsverletzer gegen Urheberrechtsinhaber ... 418
(1) Negative Feststellungsklage ... 418
(2) Analoge Anwendung der Grundsätze der Abnehmerverwarnung ... 419
cc) Ansprüche gegen den vermeintlichen Rechtsverletzer ... 420
dd) Ergebnis ... 421
g) Exkurs: Notice and Evaluation-Verfahren des BGH hinsichtlich Persönlichkeitsrechtsverletzungen ... 421
III. CACHE-PROVIDER ... 423
IV. ACCESS-PROVIDER ... 424
1. Sperrpflichten ... 425
a) Operation In Our Sites ... 426
b) Ergebnis ... 428
2. Haftung der WLAN-Betreiber ... 428
3. Warnhinweismodell ... 429
V. SONSTIGE ISP ... 430
VI. ERGEBNIS ... 432
F. SCHLUSSBETRACHTUNG UND LÖSUNGSANSÄTZE ... 432
I. VERIFIZIERUNG DER ARBEITSHYPOTHESE ... 432

II. LÖSUNGSMODELL 434
1. Anwendbarkeit auf Unterlassungsansprüche 434
a) Host-Provider 434
b) Cache-Provider 437
c) Linksetzende 438
d) Access-Provider 438
e) Änderung des TMG 440
2. Zu eigen Machen/aktiver ISP 440
3. Sonstige Providerspezifische Regelungen 442
a) Host-Provider 442
aa) Notice and Takedown-Verfahren 443
bb) Haftungsfreistellung ggü. Nutzer und Rechteinhaber 444
cc) Haftung für falsche Angaben 445
b) Cache-Provider 445
c) Access-Provider 446
d) Linksetzende und Suchmaschinenanbieter 447
aa) Suchmaschinenanbieter 447
bb) Hyperlinks 449
4. Mögliche Kritikpunkte 450
a) Anwendung der Privilegien auf Unterlassungsansprüche 450
b) Notice and Takedown-Verfahren 452
5. Vorgeschlagene Gesetzesänderung 453
6. Ausblick 458
ANHANG: AUSZUG DES § 512 DMCA 460

Abkürzungsverzeichnis

8th Cir.	United States Court of Appeals for the Eighth Circuit
a.A.	anderer Auffassung
a.F.	alte Fassung
AfP	Zeitschrift für Medien- und Kommunikationsrecht
AG	Amtsgericht
AGB	Allgemeine Geschäftsbedingungen
Alb. L. J. Sci. & Tech.	Albany Law Journal of Science & Technology
Ariz. L. Rev.	Arizona Law Review
BGB	Bürgerliches Gesetzbuch
BDSG	Bundesdatenschutzgesetz
Berkeley Tech. L.J.	Berkeley Technology Law Journal
BGH	Bundesgerichtshof
bspw.	beispielsweise
BVerfG	Bundesverfassungsgericht
bzgl.	bezüglich
Cardozo Arts & Ent. L.J.	Cardozo Arts and Entertainment Law Journal
Cardozo L. Rev	Cardozo Law Review
Case W. Reserve J.L. Tech. & Internet	Case Western Reserve Journal of Law, Technology & Internet
CCI	Center for Copyright Information
C.D. California	United States District Court for Central District of California
Colo. Tech. L. J.	Colorado Technology Law Journal
Colum. Bus. L. Rev	Columbia Business Law Review
Colum. J.L. & Arts	Columbia Journal of Law & the Arts
Colum. L. Rev.	Columbia Law Review
Computer L. Rev. & Tech. J.	Computer Law Review and Technology Journal
CR	Computer und Recht
DB	Der Betrieb

D.C. Circuit (D.C. Cir.)	United States Court of Appeals for the District of Columbia Circuit
D.C. Delaware (D. Del.)	United States District Court for the District of Delaware
d.h.	das heißt
D. Colo.	United States District Court for the District of Colorado
D. Md.	United States District Court for the District of Maryland
District Court of Nevada	United States District Court for the District of Nevada
DMCA	Digital Millenium Copyright Act
DNS	Domain Name Server
DOJ	U.S. Department of Justice
Durchsetzungs-RL	Richtlinie 2004/48/EG des Europäischen Parlaments und des Rates vom 29. April 2004 zur Durchsetzung der Rechte des geistigen Eigentums
E.D. Va.	United States District Court for the Eastern District of Virginia
ECG	Österreichische E-Commerce-Gesetz
eco	Verband der Internetwirtschaft e.V.
ECRL	Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates vom 8. Juni 2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt
EGG	Gesetz über rechtliche Rahmenbedingungen für den elektronischen Geschäftsverkehr
EIGVG	Gesetz zur Vereinheitlichung von Vorschriften über bestimmte elektronische Informations- und Kommunikationsdienste
EuGH	Europäischer Gerichtshof

EUV	Vertrag über die Europäische Union
F.Supp.2d	Federal Supplement, Second Series
F.2d	Federal Reporter, Second Series
F.3d	Federal Reporter, Third Series
FamFG	Gesetz über das Verfahren in Familiensachen und in den Angelegenheiten der freiwilligen Gerichtsbarkeit
FBI	Federal Bureau of Investigation
Fordham Intell. Prop. Media & Ent. L.J.	Fordham Intellectual Property, Media and Entertainment Law Journal
Fourth Circuit (4th Cir.)	United States Court of Appeals for the Fourth Circuit
FTP	File Transfer Protokoll
gem.	gemäß
GG	Grundgesetz
grds.	grundsätzlich
GRUR	Gewerblicher Rechtsschutz und Urheberrecht
GRURInt	Gewerblicher Rechtsschutz und Urheberrecht, Internationaler Teil
GRUR-Prax	Gewerblicher Rechtsschutz und Urheberrecht, Praxis im Immaterialgüter- und Wettbewerbsrecht
GRUR-RR	Gewerblicher Rechtsschutz und Urheberrecht Rechtsprechungs-Report
h.M.	herrschende Meinung
H. R. Rep.	House of Representatives Report
Harv. J.L. & Tech.	Harvard Journal of Law & Technology
Harv. L. Rev.	Harvard Law Review
Hastings L.J.	Hastings Law Journal
HTTP	Hypertext Transfer Protocol
ICE	Immigration and Customs Enforcement Agency
i.d.R.	in der Regel
IIC	International Review of Intellectual Property and Competition Law

IITF	Information Infrastructure Task Force
InfoSoc-RL	Richtlinie 2001/29/EG des Europäischen Parlaments und des Rates vom 22. Mai 2001 zur Harmonisierung bestimmter Aspekte des Urheberrechts und der verwandten Schutzrechte in der Informationsgesellschaft
Intell. Prop. L. Bull.	Intellectual Property Law Bulletin
IPR Center	National Intellectual Property Rights Coordination Center
i.S.d.	im Sinne des
ISP	Internet Service Provider
IuKDG	Gesetz zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste vom 22. 7. 1997 (BGBl. I S. 1870)
J. Bus. Entrepreneurship & L.	Journal of Business, Entrepreneurship & the Law
J. Copyright Soc'y U.S.A.	Journal of the Copyright Society of the U.S.A.
J. Internet L.	Journal of Internet Law
J.L. & Pol'y	Journal of Law and Policy
J. Telecomm. & High Tech. L.	Journal of Telecommunications and High Technology Law
JMStV	Jugendmedienschutz-Staatsvertrages
jurisPR-ITR	juris PraxisReport IT-Recht
KG	Kammergericht
K u. R	Kommunikation und Recht
L.A. Law.	Los Angeles Lawyer
LG	Landgericht
LMK	Kommentierte BGH-Rechtsprechung Lindenmaier-Möhring
lt.	laut
M.D.N.C.	United States District Court for the Middle District of North Carolina
MDStV	Staatsvertrag über Mediendienste
Minn. L. Rev.	Minnesota Law Review
m.M.	Mindermeinung

MMR	MultiMedia und Recht
MPAA	Motion Picture Association of America
m.w.N.	mit weiteren Nachweisen
N.C. J. L. & Tech.	North Carolina Journal of Law & Technology
N.D. California (N.D. Cal.)	United States District Court fort he Northern District of California
Nev. L.J.	Nevada Law Journal
New Eng. L. Rev.	New England Law Review
n.F.	neue Fassung
Ninth Circuit (9th Cir.)	United States Court of Appeals for the Ninth Circuit
NJ	Neue Justiz
NJW	Neue Juristische Wochenschrift
NJOZ	Neue Juristische Online Zeitschrift
N.Y.U. J. of Intell. Prop. & Ent. Law	N.Y.U. Journal of Intellectual Property and Entertainment Law
NStZ	Neue Zeitschrift für Strafrecht
OCILLA	Online Copyright Infringement Liability Limitation Act
OLG	Oberlandesgericht
Or. L. Rev.	Oregon Law Review
RIAA	Recording Industry Association of America
Rn.	Randnummer
RStV	Rundfunkstaatsvertrag
Rutgers L. Rev	Rutgers Law Review
Santa Clara Computer & High Tech. L.J.	Santa Clara High Technology Law Journal
Second Circuit (2nd Cir.)	United States Court of Appeals for the Second Circuit
Seventh Circuit	United States Court of Appeals for the Seventh Circuit
S.D.N.Y	United States District Court fort he Southern District of New York
Shidler J. L. Com & Tech.	Shidler Journal of Law, Commerce & Technology

S. Rep.	Senate Report
SMU L. Rev.	SMU Law Review
StGB	Strafgesetzbuch
St. John's J. Legal Comment.	Saint John's Journal of Legal Commentary
Stan. Tech. L. Rev.	Stanford Technology Law Review
Supreme Court (S. Ct.)	Supreme Court of the United States
Sw. U. L. Rev.	Southwestern University Law Review
TCP/IP	Transmission Control Protocol/Internet Protocol
TDG	Teledienstgesetz
Tem. J. Sci. Tech. & Envtl.	Temple Journal of Science, Technology & Environmental Law
Tex. Intell. Prop. L.J.	Texas Intellectual Property Law Journal
TKG	Telekommunikationsgesetz
TMG	Telemediengesetz
U. Miami L. Rev.	University of Miami Law Review
UCLA Ent. L. Rev.	UCLA Entertainment Law Review
UrhG	Gesetz über Urheberrechte und verwandte Schutzrechte
URL	Uniform Resource Locator
U.S.C.	Code of Laws of the United States of America
UWG	Gesetz gegen den unlauteren Wettbewerb
Vand. J. Ent. & Tech. L.	Vanderbilt Journal of Entertainment & Technology Law
Vgl.	Vergleiche
VuR	Verbraucher und Recht
WCT	WIPO Copyright Treaty
W.D. Wash.	United States District Court for the Western District of Washington
WLAN	Wireless Local Area Network
WPPT	WIPO Performances and Phonograms Treaty
WRP	Wettbewerb in Recht und Praxis
WWW	World Wide Web
z.B.	zum Beispiel
ZPO	Zivilprozessordnung

ZRP	Zeitschrift für Rechtspolitik
ZUM	Zeitschrift für Urheber- und Medienrecht
ZUM-RD	Zeitschrift für Urheber- und Medienrecht, Rechtsprechungsdienst

Literaturverzeichnis

Agress: Is There Ever a Reason to Know? A Comparison of the Contributory Liability „Knowledge“ Standard for Websites Hosting Infringed Trademarked Content Versus Infringed Copyright Content, Journal of Business, Entrepreneurship & the Law, 180-213 (2011), zit.: Agress, J. Bus. Entrepreneurship & L. 180 (2011).

Backhaus: BGH: Störerhaftung des Betreibers eines Online-Marktplatzes – „Stiftparfüm“, LMK 2011, 32613.

Ballon: E-Commerce & Internet Law: Treatise with Forms, 2. Auflage (Loseblatt-Sammlung, 2014-2015 Update), West 2009, zit.: Ballon, E-Commerce & Internet Law (2014-2015 Update).

Bartsch: Die „Vertraulichkeit und Integrität informationstechnischer Systeme“ als sonstiges Recht nach § 823 Abs. 1 BGB, CR 2008, 613-617.

Beck’scher Online-Kommentar BGB, 37. Edition, Stand: 01.11.2015, München 2015, zit.: Bearbeiter in BeckOK BGB 2015.

Beck’scher Online-Kommentar BGB, 38. Edition, Stand: 01.02.2016, München 2016, zit.: Bearbeiter in BeckOK BGB 2016.

Beck’scher Online-Kommentar, Informations- und Medienrecht, 11. Edition, Stand: 01.02.2016, zit.: Bearbeiter in BeckOK InfoMedienR.

Beck’scher Online-Kommentar StGB, 30. Edition, Stand: 01.12.2015, München, zit.: Bearbeiter in BeckOK StGB.

Beck’scher Online-Kommentar Urheberrecht, 9. Edition, Stand: 01.01.2016, München, zit.: Bearbeiter in BeckOK UrhG.

Beck’scher TKG-Kommentar, 4. Auflage, München 2013, zit.: Bearbeiter in BeckTKG-Kommentar, zit.: Bearbeiter in BeckTKG-Kommentar.

Bettinger/Freytag: Privatrechtliche Verantwortlichkeit für Links – Zugleich Anmerkung zum Urteil des LG Hamburg vom 12.5.1998, CR 1998, 545-556.

Bisges: Urheberrechtliche Aspekte des Cloud Computing – Wirtschaftlicher Vorteil gegenüber herkömmlicher Softwareüberlassung?, MMR 2012, 574-578.

Blanke: Über die Verantwortlichkeit des Internet-Providers – Eine Untersuchung anhand des Teledienstegesetzes sowie nach allgemeinen strafrechtlichen Zurechnungskategorien, Marburg 2006, zugl. : Dissertation, Hamburg 2006, zit.: Blanke.

Blevins: Uncertainty as Enforcement Mechanism: The New Expansion of Secondary Copyright Liability to Internet Platforms, 34 Cardozo Law Review, 1821-1887 (2013); zit.: Blevins, 34 Cardozo L. Rev. 1821 (2013).

Blom: Search Engines and § 512(D) of the D.M.C.A., 1 Case Western Reserve Journal of Law, Technology & Internet, 36-60 (2009), zit.: Blom, 1 Case W. Reserve J.L. Tech. & Internet 36 (2009).

Bornkamm/Seichter: Das Internet im Spiegel des UWG – Grenzwerte für die lautere Nutzung eines neuen Mediums, CR 2005, 747-753.

Bosbach/Wiege: Die strafrechtliche Verantwortlichkeit des Usenet-Betreibers nach dem Urheberrechtsgesetz, ZUM 2012, 293-299.

Bretan: Annual Review of Law and Technology: I. Intellectual Property: A. Copyright: 1. Digital Media: Harboring Doubts about the Efficacy of § 512 Immunity under the DMCA, 18 Berkeley Technology Law Journal 43-67 (2003), zit.: Bretan, 18 Berkeley Tech. L.J. 43 (2003).

Bridy: Graduated Response and the Turn to Private Ordering in Online Copyright Enforcement, 89 Oregon Law Review, 81-132 (2010), zit.: Bridy, 89 Or. L. Rev. 81 (2010).

Bridy: Is Online Copyright Enforcement Scalable?, 13 Vanderbilt Journal of Entertainment and Technology Law, 695-737 (2011), zit.: Bridy, 13 Vand. J. Ent. & Tech. L. 695 (2011).

Bridy: Graduated Response American Style: „Six Strikes“ Measured Against Five Norms, 23 Fordham Intellectual Property, Media and Entertainment Law Journal, 1-67 (2012), zit.: Bridy, 23 Fordham Intell. Prop. Media & Ent. L.J. 1 (2012).

Burnham: Introduction to the Law and Legal System of the United States, 5. Auflage, 2011, zit.: Burnham, Introduction to U.S. Law.

Carroll: Pinterest and Copyrights Safe Harbors for Internet Providers, 68 University of Miami Law Review, 421-443 (2014), zit.: Carroll, U. Miami L. Rev. 421 (2014).

Case Comment: Criminal Law – Willful Blindness – Ninth Circuit Holds that Motive is not an Element of Willful Blindness – United States v. Heredia, 483 F.3d 913 (9th Cir.) (en banc), cert. denied, 76 U.S.L.W. 3303 (U.S. Dec. 11, 2007) (No. 07-5762), 121 Harvard Law Review, 1245-1252 (2008), zit.: Case Comment, 121 Harv. L. Rev. 1245 (2008).

Case Comment: Copyright Law--Willful Blindness-- Second Circuit Holds that Willful Blindness is Knowledge in Digital Millennium Copyright Act Safe Harbor Provision.--Viacom International, Inc. v. YouTube, Inc., 676 F.3d 19 (2d Cir. 2012), 126 Harvard Law Review 645-652 (2012), zit.: Case Comment, 126 Harv. L. Rev. 645 (2012).

Center for Copyright Information: The Copyright Alert System – Phase One and Beyond, May 28, 2014, abrufbar unter http://www.copyrightinformation.org/wp-content/uploads/2014/05/Phase-One-And_Beyond.pdf, zuletzt besucht am 24.04.2016, zit.: CCI, The Copyright Alert System – Phase One and Beyond.

Chen/Durkee/Friend/Urban: Updating 17 U.S.C. § 512's Notice and Takedown Procedure for Innovators, Creators, and Consumers, March 31, 2011, abrufbar unter https://www.publicknowledge.org/documents/copyright-reform-act-notice-and-takedown, zuletzt besucht am 24.04.2016, zit.: Chen/Durkee/Friend/Urban (2011).

Chang: The Red Flag Test for Apparent Knowledge Under the DMCA § 512(c) Safe Harbor, 28 Cardozo Arts & Entertainment Law Journal 195-222 (2010), zit.: Chang, 28 Cardozo Arts & Ent. L.J. 195 (2010).

Charlesworth: The Moral of the Story: What Grokster Has to Teach About the DMCA, Stanford Technology Law Review 6, 1-61 (2011), zit.: Charlesworth, Stan. Tech. L. Rev. 6 (2011).

Civilini: Next-Generation Piracy: How Search Engines Will Destroy the Music Business, 19 UCLA Entertainment Law Review 407 – 445 (2012), zit.: Civilini, 19 UCLA Ent. L. Rev. 407 (2012).

Cohen/Loren/Okediji/O'Rourke: Copyright in a Global Information Economy, 2nd Edition, New York 2006, zit.: Cohen/Loren/Okediji/O'Rourke.

Cole: ICE Domain Name Seizures Threaten Due Process and First Amendment Rights, 20. Juni 2012, abrufbar unter https://www.aclu.org/blog/ice-domain-name-seizures-threaten-due-process-and-first-amendment-rights, zuletzt besucht am 24.04.2016, zit.: Cole, ICE Domain Name Seizures Threaten Due Process and First Amendment Rights.

Cooley: A Contractual Deterrence Strategy for User-Generated Copyright Infringement and Subsequent Service Provider Litigation, 64 SMU Law Review, 691-733 (2011), zit.: Cooley, 64 SMU L. Rev. 691 (2011).

Corwin: MegaBust's MegaQuestions Cloud the Net's Future, 13. Februar 2012, abrufbar unter http://www.circleid.com/posts/megabusts_megaquestions_cloud_the_nets_future, zuletzt besucht am 24.04.2016, zit.: Corwin, MegaBust's MegaQuestions Cloud the Net's Future.

Czychowski/Nordemann, Jan Bernd: Vorratsdaten und Urheberrecht – Zulässige Nutzung gespeicherter Daten, NJW 2008, 3095-3099, zit.: Czychowski/Nordemann, NJW 2008, 3095.

Czychowski/Nordemann: Grenzenloses Internet – entgrenzte Haftung? Leitlinien für ein Haftungsmodell der Vermittler, GRUR 2013, 986-996.

Dauner-Lieb/Langen: BGB Schuldrecht, Band 2, 2. Auflage, Bonn 2012, zit.: Bearbeiter in Dauner-Lieb/Langen.

Dietrich: Kommentar zum BGH-Urteil vom 25.10.2011 – VI ZR 93/10, NJ 2012, 200-202.

Dölling/Duttge/Rössner (Hrsg.): Gesamtes Strafrecht Handkommentar, 3. Auflage, Baden-Baden 2013, zit.: Dölling/Duttge/Rössner, Gesamtes Strafrecht.

Dreier/Schulze: Urheberrechtsgesetz Kommentar, 5. Auflage, München 2015, zit.: Bearbeiter in Dreier/Schulze.

Durner: Fernmeldegeheimnis und informationelle Selbstbestimmung als Schranken urheberrechtlicher Sperrverfügungen im Internet, ZUM 2010, 833-846.

Eck/Ruess: Haftungsprivilegierung der Provider nach der E-Commerce-Richtlinie-Umsetzungsprobleme dargestellt am Beispiel der Kenntnis nach § 11 Satz 1 Ziff. 1 TDG, MMR 2003, 363-366.

Engel-Flechsig: Das Informations- und Kommunikationsdienstegesetz des Bundes und der Mediendienstestaatsvertrag der Bundesländer – Einheitliche Rahmenbedingungen für Multimedia, ZUM 1997, 231-239.

Engel-Flechsig/Maennel/Tettenborn: Das neue Informations- und Kommunikationsdienste-Gesetz, NJW 1997, 2981-2992.

Ensthaler/Heinemann: Die Fortentwicklung der Providerhaftung durch die Rechtsprechung, GRUR 2012, 433-440.

Ernst: Anmerkung zu LG Mannheim, Beschluss vom 25.1.2007 – 7 O 65/06, MMR 2007, 538-539.

Erbs/Kohlhaas: Strafrechtliche Nebengesetze, München, Stand April 2015, zit.: Bearbeiter in Erbs/Kohlhaas.

Erfurter Kommentar zum Arbeitsrecht, 16. Auflage, München 2016, zit.: Bearbeiter in ErfK.

Falzone/Granick: Megaupload.com indictment leaves everyone guessing – Part 1, 15. März 2012, abrufbar unter http://cyberlaw.stanford.edu/publications/megauploadcom-indictment-leaves-everyone-guessing-part-1, zuletzt besucht am 24.04.2016, zit.: Falzone/Granick, Megaupload.com indictment leaves everyone guessing – Part 1.

Faustmann: Der deliktische Datenschutz, VuR 2006, 260-264.

Finlay-Hunt: Who's Leading the Blind? Aimster, Grokster, and Viacom's Vision of Knowledge in the New Digital Millennium, Columbia Business Law Review 906-960 (2013), zit.: Finley-Hunt, Colum. Bus. L. Rev. 906 (2013).

Fitzner: Sind Haftungsbeschränkungen für Host-Provider noch zeitgemäß? Der „Safe Harbor" gem. § 512 (c) Copyright Act und die Haftungsbeschränkungen gem. Art. 14 E-Commerce-Richtlinie bzw. § 10 TMG, GRURInt 2012, 109-117.

Flaim: Copyright Conspiracy: How the New Copyright Alert System May Violate the Sherman Act, 2 N.Y.U. Journal of Intellectual Property and Entertainment Law, 142-187 (2012), zit.: Flaim, 2 N.Y.U. J. of Intell. Prop. & Ent. Law 142 (2012).

Frey/Rudolph: Rechtsgutachten zur Evaluierung des „Haftungsregimes für Host- und Access-Provider im Bereich der Telemedien" im Auftrag des Bundesverband Digitale Wirtschaft (BVDW) e.V., Stand: 20. Dezember 2008, abrufbar unter http://www.bvdw.org/medien/rechtsgutachten-zum-haftungsregime-fuer-provider?media=261, zuletzt abgerufen am 24.04.2016, zit.: Frey/Rudolph, Rechtsgutachten zur Evaluierung des Haftungsregimes für Host- und Access-Provider im Bereich der Telemedien.

Frey/Rudolph/Oster: Internetsperren und der Schutz der Kommunikation im Internet – Am Beispiel behördlicher und gerichtlicher Sperrungsverfügungen im Bereich des Glücksspiel- und Urheberrechts, MMR-Beilage 3/2012, 1-26.

Frey/Rudolph/Oster: Gutachten – Rechtliche Bewertung des Gesetzentwurfs zur Neuregelung der Host-Providerhaftung, abrufbar unter https://www.eco.de/wp-content/blogs.dir/150913-gutachten-host-providerhaftung-2015000545.pdf, zuletzt besucht am 24.04.2016, zit.: Frey/Rudolph/Oster, Gutachten.

Frey, Harald: Anmerkung zum Urteil des OLG Hamburg vom 01.07.2015 - 5 U 87/12, MMR 2016, 275-277.

Freytag: Urheberrechtliche Haftung im Netz – Zur dogmatischen Einordnung und praktischen Umsetzung von § 5 TDG und § 5 MDStV bei Urheberrechtsverletzungen im Internet, ZUM 1999, 185-195.

Fuchs/Farkas: Kann der EUGH dem Paperboy das (Best)Water reichen? – Hyperlinks und Urheberrecht – zugleich Besprechung EUGH, Beschluss vom 21. Oktober 2014 – C-348/13 – BestWater, ZUM 2015, 110-126.

Gallo: The (Im)Possibility of „Standard Technical Measures“ for UGC Websites, 34 Columbia Journal of Law & the Arts, 283-315 (2011), zit.: Gallo, 34 Colum. J.L. & Arts 283 (2011).

Garner: Black’s Law Dictionary, 10th Edition, 2014, zit.: Black’s Law Dictionary.

Gercke: Anmerkung zum Urteil des LG Köln vom 04.12.2002 - 28 O 627/02, MMR 2003, 602-603.

Gercke: Die strafrechtliche Verantwortlichkeit für Hyperlinks – Warum die Verantwortlichkeitsregelungen des TDG bei einer strafrechtlichen Prüfung irrelevant sind, CR 2006, 844-850.

Ginsburg: Separating the Sony Sheep From the Grokster Goats: Reckoning the Future Business Plans of Copyright-Dependent Technology Entrepreneurs, 50 Arizona Law Review, 577-609 (2008), zit.: Ginsburg, 50 Ariz. L. Rev. 577 (2008).

Gorman: Copyright Law, 2. Auflage, Washington 2006, zit.: Gorman, Copyright Law.

Grabitz/Hilf: Das Recht der Europäischen Union
- Band IV: Sekundärrecht, 40. Ergänzungslieferung, München Oktober 2009, zit.: Bearbeiter in Grabitz/Hilf, Band IV.

Granick: Megaupload: A lot less guilty than you think, 26. Januar 2012, abrufbar unter http://cyberlaw.stanford.edu/blog/2012/01/megaupload-lot-less-guilty-you-think, zuletzt besucht am 24.04.2016, zit.: Granick, Megaupload: A lot less guilty than you think.

Grünberger: Bedarf es einer Harmonisierung der Verwertungsrechte und Schranken? – Ein Beitrag zur Entwicklung dogmatischer Bausteine eines umweltsensiblen Urheberrechts, ZUM 2015, 273-290.

Haase: Einführung in die Methodik der Rechtsvergleichung, JA 2005, 232-237.

Hacker: „L'Oréal/eBay": Die Host-Provider-Haftung vor dem EuGH, GRUR-Prax 2011, 391-393.

Haedicke: Die Haftung für mittelbare Urheber- und Wettbewerbsrechtsverletzungen - Zugleich eine Besprechung von BGH v. 15. 10. 1998 – Möbelklassiker, GRUR 1999, 397-402.

Härting: Dialer, Erotik & Rechtsberatung – Vertragsbeziehung bei 0190-Diensten, DB 2002, 2147-2150.

Härting: Anonymität und Pseudonymität im Datenschutzrecht, NJW 2013, 2065-2071.

Harder: Entertainment Law & Litigation, 2014, zit.: Entertainment Law & Litigation.

Harte-Bavendamm/Henning-Bodewig: Gesetz gegen den unlauteren Wettbewerb (UWG) – Kommentar, 3. Auflage, München 2013, zit.: Bearbeiter in Harte-Bavendamm/Henning-Bodewig.

Hay: Law of the United States, München 2002, zit.: Hay, Law of the U.S.

Helman: Pull too hard and the rope may break: On the secondary liability of technology providers for copyright infringement, 19 Texas Intellectual Property Law Journal, 111-166 (2010), zit.: Helman, 19 Tex. Intell. Prop. L.J. 111 (2010).

Helman/Parchomovsky: The Best Available Technology Standard, 111 Columbia Law Review, 1194-1243 (2011); zit.: Helman/Parchomovsky, 111 Colum. L. Rev. 1194 (2011).

Hilgendorf: Zur Anwendbarkeit des § 5 TDG auf das Strafrecht, NStZ 2000, 518-522.

Höfinger: Anmerkung zu EuGH, Urteil vom 13. Februar 2014 – C-466/12 – Nils Svensson u.a./Retriever Sverige AB, ZUM 2014, 293-295.

Högberg: The Search for Internet-based Doctrines of Secondary Liability in Copyright Law, 106 Columbia Law Review 909-958 (2006); zit.: Högberg, 106 Colum. L. Rev. 909 (2006).

Hoeren: Anmerkung zum Urteil des BGH vom 23.09.2003 – VI ZR 335/02, MMR 2004, 168-169.

Hoeren: Anmerkung zum Urteil des BGH vom 11.03.2004 – I ZR 304/01, MMR 2004, 672-673.

Hoeren: Unterlassungsansprüche gegen Host Provider – die Rechtslage nach dem Ricardo-/Rolex-Urteil des BGH, Festschrift für Ulrich Eisenhardt zum 70. Geburtstag, München 2007, 243-254, abrufbar unter http://www.uni-muenster.de/Jura.itm/hoeren/veroeffentlichungen/FS_Eisenhardt.pdf, zuletzt besucht am 24.04.2016, zit.: Hoeren in Festschrift für Ulrich Eisenhardt.

Hoeren: Anmerkung zum EuGH-Urteil vom 12.07.2011 – C-324/09, MMR 2011, 605-605.

Hoeren: Kurzgutachten zur BMWi-Studie über Modelle zur Versendung von Warnhinweisen durch Internet-Zugangsanbieter an Nutzer bei Urheberrechtsverletzungen im Auftrag des eco – Verband der deutschen Internetwirtschaft e.V., Münster, Februar 2012, abrufbar unter https://politik-recht.eco.de/wp-content/blogs.dir/20/files/20120227-hoeren-eco-gutachten_final-2702.pdf, zuletzt besucht am 24.04.2016, zit.: Hoeren, Kurzgutachten zur BMWi-Studie.

Hoeren: Anmerkung zum BGH-Urteil vom 25.10.2011 – VI ZR 93/10, MMR 2012, 127-127.

Hoeren: Anmerkung zum BGH-Urteil vom 15.08.2013 – I ZR 80/12, NJW 2013, 3245-3250.

Hoeren/Jakopp: WLAN-Haftung – A never ending story?, ZRP 2014, 72-75.

Hoeren/Sieber/Holznagel: Handbuch Multimedia-Recht – Rechtsfragen des elektronischen Geschäftsverkehrs, Loseblatt-Ausgabe, 42. Ergänzungslieferung, München, Juni 2015, zit.: Bearbeiter in Hoeren/Sieber/Holznagel.

Hoeren/Yankova: The Liability of Internet Intermediaries – The German Perspective, IIC 2012, 501-531.

Hoffmann: Zivilrechtliche Haftung im Internet, MMR 2002, 284-289.

Hofmann: Markenrechtliche Sperranordnungen gegen nicht verantwortliche Intermediäre – Das englische „Cartier"-Urteil und seine Lehren für das deutsche Recht, GRUR 2015, 123-130.

Hofmann: Störerhaftung von Access-Providern für Urheberrechtsverletzungen Dritter, NJW 2016, 796-771.

Hollenders: Mittelbare Verantwortlichkeit von Intermediären im Netz, Baden-Baden 2012, zugl. Dissertation, Münster 2011, zit.: Hollenders.

Holznagel: Zur Providerhaftung – Notice and Take-Down in § 512 U.S. Copyright Act, GRUR Int 2007, 971-986.

Holznagel: Die Urteile in Tiffany v. eBay (USA) – zugleich zu aktuellen Problemen der europäischen Providerhaftung, GRUR Int 2010, 654-663.

Holznagel: Notice and Take-Down-Verfahren als Teil der Providerhaftung, Tübingen 2013, zugl. Dissertation, Göttingen 2010, zit.: Holznagel.

Holznagel: Melde- und Abhilfeverfahren zur Beanstandung rechtwidrig gehosteter Inhalte nach europäischem und deutschem Recht im Vergleich zu gesetzlich geregelten notice and

take-down-Verfahren – Zugleich zur „notice and action“ Initiative der EU-Kommission sowie zur Blog-Eintrag-Entscheidung des BGH, GRUR Int 2014, 105-114.

Jani/Leenen: Anmerkung zum EuGH-Urteil vom 13.02.2014 – C-466/12, GRUR 2014, 362-363.

Karg: IP-Adressen sind personenbezogene Verkehrsdaten, MMR-Aktuell 2011, 315811.

Kartal-Aydemir/Krieg: Haftung von Anbietern kollaborativer Internetplattformen – Störerhaftung für User Generated Content?, MMR 2012, 647-652.

Killian/Heussen: Computerrechts-Handbuch – Informationstechnologie in der Rechts- und Wirtschaftspraxis, Loseblatt, 32. Ergänzungslieferung, München August 2013, zit.: Bearbeiter in Kilian/Heussen.

Klatt: Die Kerngleichheit als Grenze der Prüfungspflichten und der Haftung des Hostproviders, ZUM 2009, 265-274.

Klemchuk/Jones: How Quickly Do Internet Companies Need to Take Content Down Following a DMCA Notice?, 18 No. 10 Journal of Internet Law 1, 35-38 (2015), zit.: Klemchuck/Jones, 18 No. 10 J. Internet L.1, 35 (2015).

Koch: Haftung für die Weiterverbreitung von Viren durch E-Mails, NJW 2004, 801-806.

Köhler/Bornkamm: Gesetz gegen den unlauteren Wettbewerb, 34. Auflage, München 2016, zit.: Bearbeiter in Köhler/Bornkamm.

Kopel: Operation Seizing Our Sites: How the Federal Government is Taking Domain Names Without Prior Notice, 28 Berkeley Technology Law Journal (2013), 859-900, zit.: Kopel, 28 Berkeley Tech. L.J. 859 (2013).

Kopko: Looking for a Crack to Break the Internet’s Back: The Listen4ever Case and Backbone Provider Liability Under the Copyright Act and the DMCA, 8 Computer Law

Review & Technology Journal 83-117 (2003), zit.: Kopko, 8 Computer L. Rev. & Tech. J. 83 (2003).

Krüger/Apel: Haftung von Plattformbetreibern für urheberrechtlich geschützte Inhalte – Wie weit geht die Haftung und wann droht Schadensersatz?, MMR 2012, 144-151.

Ladeur: Der Auskunftsanspruch aus § 101 UrhG und seine Durchsetzung – Zivilrechtsanwendung ohne Methode und jenseits der Drittwirkung der Grundrechte?, NJW 2010, 2702-2702.

Leaffer: Understanding Copyright Law, 6th Edition, 2014, zit.: Leaffer.

Lee: Decoding the DMCA Safe Harbors, 32 Columbia Journal of Law & the Arts, 233-269 (2009), zit.: Lee, 32 Colum. J.L. & Arts 233 (2009).

Leible/Sosnitza: Neues zur Störerhaftung von Internet-Auktionshäusern, NJW 2004, 3225-3227.

Leistner: Von „Grundig-Reporter(n) zu Paperboy(s)“ – Entwicklungsperspektiven der Verantwortlichkeit im Urheberrecht, GRUR 2006, 801-814.

Leistner: Grundlagen und Perspektiven der Haftung für Urheberrechtsverletzungen im Internet, ZUM 2012, 722-740.

Leistner: Urheberrecht an der Schnittstelle zwischen Unionsrecht und nationalem Recht, GRUR 2014, 1145-1155.

Leistner/Grisse: Sperrverfügungen gegen Access-Provider im Rahmen der Störerhaftung (Teil 1), GRUR 2015, 19-27.

Lemley: Rationalizing Internet Safe Harbors, 6 Journal on Telecommunications & High Technology Law, 101-119 (2007), zit.: Lemley, 6 J. Telecomm. & High Tech. L. 101 (2007).

Leupold/Glossner: Münchener Anwalts Handbuch IT-Recht, 3. Auflage, München 2013, zit.: Bearbeiter in Leupold/Glossner.

Lessig: Affidavit of Lawrence Lessig dated September 2015 in the matter Proceedings to extradite Kim Dotcom, Bram van der Kolk, Finn Habib Batato and Mathias Ortmann, 14. September 2015, abrufbar unter http://static1.1.sqspcdn.com/static/f/201542/26539482/1442342840337/LessigKimDotcomRothkenLaw.pdf?token=3bTLPEf9lBrcHxYggl3%2BWuM9Dh0%3D, zuletzt besucht am 24.04.2016, zit.: Lessig, Expert Opinion.

Liu: Why Is Betamax an Anachronism in the Digital Age? Erosion of the Sony Doctrine and Indirect Copyright Liability of Internet Technologies, Vanderbilt Journal of Entertainment and Technology Law, Vol. 7, 343-366 (2005), zit.: Liu, Vanderbilt Journal of Entertainment and Technology Law, 343 (2005).

Loewenheim: Handbuch des Urheberrechts, 2. Auflage, München 2010, zit.: Bearbeiter in Loewenheim.

Lorenz: Anwendbarkeit der Haftungsprivilegierung gemäß § 10 TMG auf Unterlassungsansprüche gegen Internetauktionshaus („Stiftparfum“), jurisPR-ITR 6/2012 Anm. 4.

Lovejoy: Standards for Determining when ISPs have fallen out of Section 512 (a), 27 Harvard Journal of Law & Technology 257-277 (2013), zit.: Lovejoy, 27 Harv. J.L. & Tech. 257 (2013).

Ludwig: Shooting the Messenger: ISP Liability for Contributory Copyright Infringement, Boston College Intellectual Property & Technology Forum, 1-19 (2006), zit.: Ludwig, Boston College Intellectual Property & Technology Forum (2006).

Manta: The Puzzle of Criminal Sanctions for Intellectual Property Infringements, Harvard Journal of Law and Technology, Volume 24, Number 2, 469-518 (2011), zit.: Manta, 24 Harv. J.L. & Tech. 469 (2011).

Mantz: Anmerkung zu LG Hamburg, Urteil vom 26.7.2006 – 308 O 407/06, MMR 2006, 764-766.

Mantz/Gietl: Anmerkung zu OLG Frankfurt, Urteil vom 1.7.2008 – 11 U 52/07, MMR 2008, 606-609.

Mantz: Anmerkung zu BGH, Urteil vom 12.5.2010 – I ZR 121/08, MMR 2010, 568-570.

Mantz: Die Haftung des Betreibers eines gewerblich betriebenen WLANs und die Haftungsprivilegierung des § 8 TMG – Zugleich Besprechung von LG Frankfurt a.M., Urt. v. 28.6.2013 – 2-06 O 304/12 – Ferienwohnung, GRUR-RR 2013, 497-500.

Mantz/Sassenberg: Verantwortlichkeit des Access-Providers auf dem europäischen Prüfstand – Neun Fragen an den EuGH zu Haftungsprivilegierung, Unterlassungsanspruch und Prüfpflichten des WLAN-Betreibers, MMR 2015, 85-90.

Marly: Anmerkung zum Urteil des EuGH vom 27.03.2014 - C-314/12, GRUR 2014, 472-473.

Martin/Newhall: Criminal Copyright Enforcement Against Filesharing Services, North Carolina Journal of Law and Technology, Volume 15, 101-151 (2013), zit.: Martin/Newhall, 15 N.C. J. L. & Tech. 101 (2013).

Mazoki: Viacom International Inc. v. YouTube Inc. and the Failings of the Southern District Court of New York, 30 Temple Journal of Science, Technology & Environmental Law 275-310 (2011), zit.: Mazoki, 30 Tem. J. Sci. Tech. & Envtl. L. 275 (2011).

McMahon: The Digital Millennium Copyright Act and the Directive on Electronic Commerce Offer Similar Protections to ISPs, 37 Los Angeles Lawyer, 28-33 (2014), zit.: McMahon, 37 L.A. Law. 28 (2014).

Meier/Wehlau: Die zivilrechtliche Haftung für Datenlöschung, Datenverlust und Datenzerstörung, NJW 1998, 1585-1591.

Miles: In re Aimster & MGM, Inc. v. Grokster, Ltd.: Peer-to-Peer and the Sony Doctrine, 19 Berkeley Technology Law Journal (2004), 21-57, zit.: Miles, 19 Berkeley Tech. L.J. 21 (2004).

Minnock: Should Copyright Laws Be Able to Keep Up With Online Piracy?, Colorado Technology Law Journal, 523-552 (2014), zit.: Minnock, Colo. Tech. L. J. 523 (2014).

Mlynar: A Storm in ISP Safe Harbor Provisions: The Shift from Requiring Passive-Reactive to Active-Preventative Behavior and Back, 19 Intellectual Property Law Bulletin, 1-27 (2014), zit.: Mlynar, 19 Intell. Prop. L. Bull. 1 (2014).

Mtima: Whom the Gods Would Destroy: Why Congress Prioritized Copyright Protection Over Internet Privacy in Passing the Digital Millenium Copyright Act, 61 Rutgers Law Review, 627-704 (2009), zit.: Mtima, 61 Rutgers L. Rev. 627 (2009).

Müller-Broich: Telemediengesetz, Baden-Baden 2012, zit.: Müller-Broich.

Münchener Kommentar zum BGB
- Band 2, Schuldrecht - Allgemeiner Teil, 7. Auflage 2016,
- Band 5, Schuldrecht Besonderer Teil III, §§ 705-853, Partnerschaftsgesellschaftsgesetz, Produkthaftungsgesetz, 6. Auflage, München 2013,
zit.: Bearbeiter in MüKo BGB.

Münchener Kommentar zum StGB
- Band 7: Nebenstrafrecht II, 2. Auflage, München 2015,
zit.: Bearbeiter in MüKo zum StGB.

Murtagh: The FCC, the DMCA, and Why Takedown Notices Are Not Enough, 61 Hastings Law Journal, 233-273 (2009), zit.: Murtagh, 61 Hastings L.J. 233 (2009).

Musielak/Voit (Hrsg.): Zivilprozessordnung mit Gerichtsverfassungsgesetz – Kommentar, 13. Auflage, München 2016, zit.: Bearbeiter in Musielak/Voit, ZPO.

Nazari-Khanachayi: Access-Provider als urheberrechtliche Schnittstelle im Internet - Europarechtliche Vorgaben im Hinblick auf Zugangserschwerungsverfügungen und Lösungsansätze für das deutsche Recht de lege ferenda, GRUR 2015, 115-122.

Nimmer: Copyright Illuminated – Refocusing the Diffuse US Statute, Alphen aan den Rijn, 2008, zit.: Nimmer, Copyright Illuminated.

Nimmer/Nimmer: Nimmer on Copyright, Loseblatt-Sammlung, Stand Mai 2015, zit.: Nimmer on Copyright.

Nolte, Georg/Wimmers: Wer stört? Gedanken zur Haftung von Intermediären im Internet – Von praktischer Konkordanz, richtigen Anreizen und offenen Fragen, GRUR-Beilage 2014, 58-69.

Nordemann, Jan Bernd: Haftung von Providern im Urheberrecht – Der aktuelle Stand nach dem EuGH-Urteil v. 12.7.2011 – C-324/09 – L'Oréal/eBay, GRUR 2011, 977-981.

Nordemann, Jan Bernd: Anmerkung zu EuGH, Urteil vom 27. März 2014 – C-314/12 – UPC Telekabel Wien GmbH/Constantin Film Verleih GmbH, Wega Filmproduktionsgesellschaft mbH („Kino.to"), ZUM 2014, 499-501.

Ohly: Keyword Advertising auf dem Weg zurück von Luxemburg nach Paris, Wien, Karlsruhe und Den Haag, GRUR 2010, 776-785.

Ohly: Die Verantwortlichkeit von Intermediären, ZUM 2015, 308-318.

Ott: Die Haftung von YouTube für urheberrechtsverletzende Uploads seiner Nutzer nach US-amerikanischem Recht, GRUR Int 2008, 563-569.

Peguera: When the Cached Link is the Weakest Link: Search Engine Caches under the Digital Millenium Copyright Act, 56 Journal of the Copyright Society in the U.S.A. 589 – 645 (2009), Part I, zit.: Peguera, 56 J. Copyright Soc'y U.S.A. 589 (2009).

Peifer: Konvergenz in der Störer- und Verbreiterhaftung – Vom Störer zum Verbreiter?, AfP 1/2014, 18-23.

Pfitzmann/Köpsell/Kriegelstein: Sperrverfügungen gegen Access-Provider – Technisches Gutachten, TU Dresden, 2008, abrufbar unter http://www.kjm-online.de/fileadmin/Download_KJM/Service/Gutachten/Gutachten_Sperrverfuegung_Technik_2008.pdf, zuletzt besucht am 24.04.2016, zit.: Pfitzmann/Köpsell/Kriegelstein, Sperrverfügungen gegen Access-Provider.

Pollack: Rebalancing Section 512 to Protect Fair Users from Herds of Mice - Trampling Elephants, or a Little Due Process Is Not Such a Dangerous Thing, 22 Santa Clara High Technology Law Journal, 547-576 (2005), zit.: Pollack, 22 Santa Clara High Tech. L.J. 547 (2005).

Popescu: Verschuldensabhängige Störerhaftung für den unzureichend gesicherten WLAN-Anschluss, VuR 2011, 327-333.

Rasenberger/Pepe: Copyright Enforcement and Online File Hosting Services: Have Courts Struck the Proper Balance?, 59 Journal of the Copyright Society of the U.S.A., 627-693 (2012), zit.: Rasenberger/Pepe, 59 J. Copyright Soc'y U.S.A., 627 (2012).

Rauer: Anmerkung zum BGH-Urteil vom 12.07.2012 – I ZR 18/11, GRUR-Prax 2013, 93-93.

Redeker: IT-Recht, 5. Auflage, München 2012, zit.: Redeker, IT-Recht.

Reese: Comment: Wading through the Muddy Waters: The Courts' Misapplication of Section 512(c) of the Digital Millenium Copyright Act, 34 Southwestern University Law Review 287-323 (2004), zit.: Reese, 34 Sw. U. L. Rev. 287 (2004).

Reese: The Relationship Between the ISP Safe Harbors and the Ordinary Rules of Copyright Liability, 32 Columbia Journal of Law and the Arts 427-443 (2009), zit.: Reese, 32 Colum. J. L. & Arts 427 (2009).

Reiley/de la Vega: The American Legal System for Foreign Lawyers, New York 2012, zit.: Reiley/de la Vega.

Reinbacher: Zur Strafbarkeit der Betreiber und Nutzer von Kino.to – zugleich eine Anmerkung zu LG Leipzig, Urt. v. 16.6.2012, Az.: 11 KLs 390 Js 191/11 = ZUM 2013, 338, NStZ 2014, 57-62.

Rempe: Anmerkung zum Urteil des OLG Hamburg vom 13.5.2013 – 5 W 41/13, MMR 2013, 534-535.

Rozsnyai: Easy Come, Easy Go: Copyright Infringement and the DMCA's Notice and Takedown Provision in Light of Rossi v. MPAA, 2 Shidler Journal of Law, Commerce & Technology 15 (2006), zit.: Rozsnyai, 2 Shidler J. L. Com & Tech. 15 (2006).

Rühl: Anmerkung zum BGH-Urteil vom 25.10.2011 – VI ZR 93/10, LMK 2012, 338417.

Satzger: Strafrechtliche Verantwortlichkeit von Zugangsvermittlern – Eine Untersuchung der Verantwortlichkeit für rechtswidrige Inhalte im Internet vor dem Hintergrund der neuen E-Commerce-Richtlinie der EG, CR 2001, 109-117.

Schachter: Substantially Perfect: The Southern District of New York's Problematic Rewrite of the DMCA' Elements of Notification, 29 Cardozo Arts and Entertainment Law Journal, 495-521 (2011), zit.: Schachter, 29 Cardozo Arts & Ent. L.J. 495 (2011).

Schnabel/Freund: „Ach wie gut, dass niemand weiß..." – Selbstdatenschutz bei der Nutzung von Telemedienangeboten, CR 2010, 718-721.

Schneidman: The Coypright Alert System: A Potential Unfair Burden on Small Business Owners, 23 Journal of Law and Policy, 397-447 (2014), zit.: Schneidman, 23 J.L. & Pol'y 397 (2014).

Schönke/Schröder: Strafgesetzbuch Kommentar, 29. Auflage, München 2014, zit.: Bearbeiter in Schönke/Schröder.

Schulze: Rechtsfragen von Printmedien im Internet, ZUM 2000, 432-455.

Schulze: Svensson, BestWater und Die Realität – Ist Framing nun grundsätzlich zulässig? – Anmerkung zu EuGH, Beschluss vom 21. Oktober 2014 – C-348/13 – BestWater, ZUM 2015, 106-110.

Schwartmann: Vergleichende Studie über Modelle zur Versendung von Warnhinweisen durch Internet-Zugangsanbieter an Nutzer bei Urheberrechtsverletzungen im Auftrag des Bundesministeriums für Wirtschaft und Technologie, I C 4-02 08 15-29/11, Januar 2012, einsehbar unter http://www.bmwi.de/DE/Mediathek/publikationen,did=474202.html, zuletzt besucht am 24.04.2016, zit.: Schwartmann, Vergleichende Studie über Modelle zur Versendung von Warnhinweisen.

Scott: Scott on Multimedia Law, 3rd Edition (Loseblatt-Sammlung, 2014 Supplement), zit.: Scott on Multimedia Law.

Scott: Scott on Information Technology (CCH), 3rd Edition (Loseblatt-Sammlung, 2014 Supplement), zit.: Scott on Information Technology.

Sieber: Anmerkung zum Urteil des AG München vom 28.05.1998, MMR 1998, 438-448.

Sieber: Verantwortlichkeit im Internet - Technische Kontrollmöglichkeiten und multimediarechtliche Regelungen, München 1999, zit.: Sieber.

Sirichit: Catching the Conscience: An Analysis of the knowledge theory under § 512 (c)'s Safe Harbor & the Role of Willful Blindness in the Finding of Red Flags, 23 Albany Law Journal of Science & Technology, 85-190 (2013), zit.: Sirichit, 23 Alb. L. J. Sci. & Tech. 85 (2013).

Sobola/Kohl: Haftung von Providern für fremde Inhalte – Haftungsprivilegierung nach § 11 TDG – Grundsatzanalyse und Tendenzen der Rechtsprechung, CR 2005, 443-450.

Solmecke: Anmerkung zum EuGH-Urteil vom 21.12.2014 – C-348/13, MMR 2015, 48.

Spindler: Haftungsrechtliche Grundprobleme der neuen Medien, NJW 1997, 3193-3199.

Spindler: Die zivilrechtliche Verantwortlichkeit von Internetauktionshäusern – Haftung für automatisch registrierte und publizierte Inhalte?, MMR 2001, 737-743.

Spindler: Anmerkung zum BGH-Urteil vom 23.09.2003 – VI ZR 335/02, CR 2004, 50-51.

Spindler: Anmerkung zum Urteil des OLG Brandenburg vom 16.12.2003 – 6 U 161/02, MMR 2004, 333-334.

Spindler: Die Verantwortlichkeit der Provider für „Sich-zu-Eigen-gemachte“ Inhalte und für beaufsichtigte Nutzer, MMR 2004, 440-444.

Spindler/Leistner: Die Verantwortlichkeit für Urheberrechtsverletzungen im Internet – Neue Entwicklung in Deutschland und in den USA, GRUR Int 2005, 773-796.

Spindler: Anmerkung zum Urteil des OLG Hamburg vom 08.02.2006 – 5 U 78/05, MMR 2006, 403-405.

Spindler: Anmerkung zum BGH-Urteil vom 19.04.2007 – I ZR 35/04, MMR 2007, 511-514.

Spindler: „Die Tür ist auf“ – Europarechtliche Zulässigkeit von Auskunftsansprüchen gegenüber Providern, Urteilsanmerkung zu EuGH „Promusicae/Telefónica“, GRUR 2008, 574-577.

Spindler: Europarechtliche Rahmenbedingungen der Störerhaftung im Internet – Rechtsfortbildung durch den EuGH in Sachen L’Oréal/eBay, MMR 2011, 703-707.

Spindler: Anmerkung zum BGH-Urteil vom 19.10.2011 – I ZR 140/10, MMR 2012, 386-387.

Spindler: Zivilrechtliche Sperrverfügungen gegen Access-Provider nach dem EuGH-Urteil „UPC Telekabel“, GRUR 2014, 826-834.

Spindler/Schuster: Recht der elektronischen Medien, 3. Auflage, München 2015, zit.: Bearbeiter in Spindler/Schuster.

Spindler: Das Ende der Links: Framing und Hyperlinks auf rechtswidrige Inhalte als eigenständige Veröffentlichung?, GRUR 2016, 157-160.

Stang/Hühner: Haftung des Anschlussinhabers für fremde Rechtsverletzungen beim Betrieb eines ungesicherten WLAN-Funknetzes – Zugleich Anmerkung zu OLG Frankfurt a.M., GRUR-RR 2008, 279 – Ungesichertes WLAN, GRUR-RR 2008, 273-275.

Stang/Hühner: Anmerkung zu BGH, Urteil vom 12.5.2010 – I ZR 121/08 Sommer unseres Lebens, GRUR 2010, 636-637.

Storch: Copyright Vigilantism, 16 Stanford Technology Law Review, 453-483 (2013), zit.: Storch, 16 Stan. Tech. L. Rev. 453 (2013).

Tettenborn: Die Evaluierung des IuKDG – Erfahrungen, Erkenntnisse und Schlussfolgerungen, MMR 1999, 516-522.

Tettenborn/Bender/Lübben/Karenfort/Santelmann/Enaux/König: Rechtsrahmen für den elektronischen Geschäftsverkehr, K u. R 2001, Beilage 1-40.

Thum: Schlichte Einwilligung zu Google-Thumbnails wirkt abstrakt-generell – „Vorschaubilder II“, GRUR-Prax 2012, 215-216.

Urban/Quilter: Symposium Review: Efficient Process or „Chilling Effects“? Takedown Notices Under Section 512 of The Digital Millennium Copyright Act, 22 Santa Clara Computer & High Technology Law Journal, 621-693 (2006), zit.: Urban/Quilter, 22 Santa Clara Computer & High Tech. L.J. 621 (2006) .

Vassilaki: Strafrechtliche Haftung nach §§ 8 ff. TDG, MMR 2002, 659-662.

Villalón: Schlussanträge vom 26.11.2013 - UPC Telekabel Wien - Rechtssache C-314/12, BeckEuRS 2013, 743182.

Völzmann-Stickelbrock: Anmerkung zum BGH-Urteil vom 15.08.2013 – I ZR 80/12, LMK 2013, 352737.

von der Groeben/Schwarze/Hatje: Europäisches Unionsrecht, 7. Auflage, Baden-Baden 2015, zit.: Bearbeiter in von der Groeben/Schwarze/Hatje.

von Ungern-Sternberg: Die Rechtsprechung des Bundesgerichtshofs zum Urheberrecht und zu den verwandten Schutzrechten in den Jahren 2010 und 2011 (Teil II), GRUR 2012, 321-331.

Wabnitz/Janovsky (Hrsg.): Handbuch des Wirtschafts- und Steuerstrafrechts, 4. Auflage, München 2014, zit.: Bearbeiter in Wabnitz/Janovsky.

Waldenberger: Teledienste, Mediendienste und die „Verantwortlichkeit“ ihrer Anbieter, MMR 1998, 124-129.

Waldenberger: Anmerkung zum Urteil des OLG München vom 08.03.2001 – 29 U 3282/00, MMR 2001, 378-379.

Walker: Application of the DMCA Safe Harbor Provisions to Search Engines, Viginia Journal of Law & Technology, University of Virginia, Vol. 9 No. 2, (2004), zit.: Walker, Virginia Journal of Law & Technology Vol. 9, No.2 (2004).

Wandtke/Bullinger: Praxiskommentar zum Urheberrecht, 4. Auflage, München 2014, zit.: Bearbeiter in Wandtke/Bullinger.

Watkins: Wireless Liability: Liability Concerns for Operators of Unsecured Wireless Networks, 65 Rutgers Law Review, 635 (2013), abrufbar unter http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2035633##, zuletzt besucht am 24.04.2016, zit.: Watkins, Wireless Liability (2013).

Weinstein: Defining Expeditious: Unchartered Territory of the DMCA Safe Harbor Provision – A Survey of What We Know and Do Not Know About the Expeditiousness of Service

Provider Responses to Takedown Notifications, 26 Cardozo Arts & Entertainment Law Journal, 589-621 (2008), zit.: Weinstein, 26 Cardozo Arts & Ent. L.J. 598 (2008).

Westphalen, Graf von: Vertragsrecht und AGB-Klauselwerke, 36. Ergänzung, München 2015, zit.: Bearbeiter in Westphalen, Graf von, Vertragsrecht.

Wiebe: Providerhaftung in Europa: Neue Denkanstöße durch den EuGH, Teil 1: Die Haftung der Host-Provider nach der bisherigen Rechtsprechung des BGH Und der Vorabentscheidung des EuGH in der Rechtssache L'Oréal ./. eBay, WRP 2012, 1182-1189.

Williams: The Second Circuit Up Some Knowledge in Viacom v. YouTube, 48 New England Law Review, 657-677 (2014), zit.: Williams, 48 New Eng. L. Rev. 657 (2014).

Wiseman: Limiting Innovation Through Willful Blindness, 14 Nevada Law Journal, 210-235 (2013), zit.: Wiseman, 14 Nev. L.J. 210 (2013).

White: Viacom v. YouTube: A Proving Ground for DMCA Safe Harbors against Secondary Liability, 24 Saint John's Journal of Legal Commentary, 811-850 (2010), zit.: White, 24 St. John's J. Legal Comment. 811 (2010).

Yen: Third-Party Copyright Liability After Grokster, 91 Minnesota Law Review, 184-240 (2006), zit.: Yen, 91 Minn. L. Rev. 184 (2006).

Zech: „Industrie 4.0" – Rechtsrahmen für eine Datenwirtschaft im digitalen Binnenmarkt, GRUR 2015, 1151-1160.

Sonstige Quellen

achatech/BDI/Fraunhofer/ZEW: Innovationsindikator 2015, abrufbar unter http://www.innovationsindikator.de/fileadmin/2015/PDF/Innovationsindikator_2015_Web.pdf, zuletzt besucht am 24.04.2016, zit.: Innovationsindikator 2015.

Bitcom: Stellungnahme – Referentenentwurf eines 2. Gesetzes zur Änderung des Telemediengesetzes (2. TMGÄndG, in der Fassung vom 15. Juni 2015), 15. Juli 2015, abrufbar unter: https://www.bitkom.org/Publikationen/2015/Positionspapiere/Stellungnahme-

Referentenentwurf-zum-Telemediengesetz-TMGAendG/20150715_Bitkom_Stellungnahme_Telemediengesetz_Zweiter_RefE_FINAL.pdf, zuletzt besucht am 24.04.2016, zit.: Bitkom, Stellungnahme zur Änderung des TMG.

Briegleb: Justizministerin: Three Strikes „mit mir nicht“, 22.08.2012, abrufbar unter http://www.heise.de/newsticker/meldung/Justizministerin-Three-Strikes-mit-mir-nicht-1673008.html, zuletzt besucht am 21.08.16, zit.: Briegleb: Justizministerin: Three Strikes „mit mir nicht“.

Bundesregierung: Gesetzentwurf - Entwurf eines Zweiten Gesetzes zur Änderung des Telemediengesetzes, abrufbar unter http://www.bmwi.de/BMWi/Redaktion/PDF/S-T/telemedienaenderungsgesetz-aenderung,property=pdf,bereich=bmwi2012,sprache=de,rwb=true.pdf, zuletzt besucht am 24.04.2016, zit.: Gesetzentwurf zur Änderung des TMG.

Center for Copyright Information: Memorandum of Understanding, abrufbar unter http://www.copyrightinformation.org/wp-content/uploads/2013/02/Memorandum-of-Understanding.pdf, zuletzt besucht am 24.04.2016, zit.: Memorandum of Understanding.

Cieply: Small Film Producers Form a Group to Counter Privacy, abrufbar unter http://www.nytimes.com/2015/04/20/business/media/small-film-producers-form-a-group-to-counter-piracy.html?ref=technology&_r=2, zuletzt besucht am 24.04.2016, zit.: Cieply, Small Film Producers Form a Group to Counter Privacy.

Digitale Gesellschaft e.V.: A clean and open Internet: Public consultation on procedures for notifying and acting on illegal content hosted by online intermediaries, abrufbar unter https://pound.netzpolitik.org/wp-upload/N_a_T_answers_digiges.pdf, zuletzt besucht am 24.04.2016, zit.: Digitale Gesellschaft, Public consultation.

Google: Beantwortung der „Fragen zur Regelungen der Anbieterhaftung im Telemediengesetz (TMG) (Fragebogen des Bundesministeriums für Wirtschaft und Technologie), abrufbar unter http://www.gesmat.bundesgerichtshof.de/gesetzesmaterialien/16_wp/elgvg/stellung_fragkat_google.pdf, zuletzt besucht am 24.04.2016, zit.: Google, Stellungnahme zur Anbieterhaftung.

H. Con. Res. 190 des 110ten Kongresses: „How our laws are made“, abrufbar unter http://www.gpo.gov/fdsys/pkg/CDOC-110hdoc49/pdf/CDOC-110hdoc49.pdf, zuletzt besucht am 24.04.2016, zit

Harmon: „Notice-and-Stay-Down“ Is Really „Filter-Everything“, January 21, 2016, abrufbar unter https://www.eff.org/de/deeplinks/2016/01/notice-and-stay-down-really-filter-everything, zuletzt besucht am 24.04.2016, zit.: Harmon.

House of Representatives, 105th Congress, 2d Session, Report 105-796, Conference Report [to accompany H.R. 2281], abrufbar unter https://www.gpo.gov/fdsys/pkg/CRPT-105hrpt796/pdf/CRPT-105hrpt796.pdf, zuletzt besucht am 24.04.2016, zit.: Conference Report.

H.R.2180 - 105th Congress (1997-1998) to amend title 17, United States Code, to provide limitations on copyright liability relating to material on-line, and for other purposes, abrufbar unter https://www.congress.gov/105/bills/hr2180/BILLS-105hr2180ih.pdf, zuletzt besucht am 24.04.2016, zit.: H.R. 2180.

H.R. REP. 105-551(I), 105TH Cong., 2ND Sess. 1998, 1998 WL 261605 (Leg.Hist.)
P.L. 105-304, DIGITAL MILLENNIUM COPYRIGHT ACT, abrufbar unter https://www.congress.gov/105/crpt/hrpt551/CRPT-105hrpt551-pt1.pdf, zuletzt besucht am 24.04.2016, zit.: H.R. Rep. 105-551(I).

H.R. REP. 105-551(II), 105TH Cong., 2ND Sess. 1998, 1998 WL 414916 (Leg.Hist.)
P.L. 105-304, DIGITAL MILLENNIUM COPYRIGHT ACT OF 1998, abrufbar unter https://www.congress.gov/105/crpt/hrpt551/CRPT-105hrpt551-pt2.pdf, zuletzt besucht am 24.04.2016, zit.: H.R. Rep. 105-551(II).

Information Infrastructure Task Force, Intellectual Property and the National Information Infrastructure, The Report of the Working Group on Intellectual Property Rights, September 1995, abrufbar unter http://www.uspto.gov/web/offices/com/doc/ipnii/ipnii.pdf, zuletzt besucht am 24.04.2016, zit.: Information Infrastructure Task Force.

Johnson: Producers' Coalition Says Copyright Alert System Has Failed to Stop Piracy, abrufbar unter http://variety.com/2015/biz/news/copyright-alert-system-piracy-expendables-3-1201493788/, zuletzt besucht am 24.04.2016, zit.: Johnson: Producers' Coalition Says Copyright Alert System Has Failed to Stop Piracy.

Koalitionsvertrag der CDU, CSU und FPD, 17. Legislaturperiode, abrufbar unter http://www.bmi.bund.de/SharedDocs/Downloads/DE/Ministerium/koalitionsvertrag.pdf;jsessionid=511E7ABEA5CC66CCB46B01D22E3246D5.2_cid373?__blob=publicationFile, zuletzt besucht am 24.04.2016, zit.: Koalitionsvertrag von CDU, CSU und FDP.

Koalitionsvertrag der CDU, CSU und SPD, 18. Legislaturperiode, abrufbar unter http://www.bundesregierung.de/Content/DE/_Anlagen/2013/2013-12-17-koalitionsvertrag.pdf;jsessionid=99FCB1185969B729842D1499241E7829.s3t2?__blob=publicationFile&v=2, zuletzt besucht am 24.04.2016, zit.: Koalitionsvertrag von CDU, CSU und SPD.

Konrad Adenauer Stiftung: Start-ups in Deutschland und den USA, Analysen & Argumente, Ausgabe 99, November 2011, abrufbar unter http://www.kas.de/wf/doc/kas_29348-544-1-30.pdf?160114114853, zuletzt besucht am 24.04.2016, zit.: Start-ups in Deutschland und den USA.

Lesser: Copyright Alert System Set to Begin, 25. Februar 2013, abrufbar unter http://www.copyrightinformation.org/uncategorized/copyright-alert-system-set-to-begin/, zuletzt besucht am 24.04.2016, zit.: Lesser, Copyright Alert System Set to Begin.

McGee: Yahoo Closes European Directories, Says US Directory Is Safe, 17. Juni 2010, abrufbar unter http://searchengineland.com/yahoo-closes-european-directories-us-directory-safe-44610, zuletzt besucht am 24.04.2016, zit.: McGee, Yahoo Closes European Directories.

Rangnath: The McCain Campaign's Run In With The DMCA Highlights Need For More Balanced Copyright Law, October 16, 2008, abrufbar unter https://www.publicknowledge.org/news-blog/blogs/the-mccain-campaigns-run-in-with-the-dmca-highlights-need-for-more-balanced, zuletzt besucht am 24.04.2016, zit.: Rangnath, The

McCain Campaign's Run In With The DMCA Highlights Need For More Balanced Copyright Law.

S.1146 - 105th Congress (1997-1998) to amend title 17, United States Code, to provide limitations on copyright liability relating to material on-line, and for other purposes, abrufbar unter https://www.congress.gov/105/bills/s1146/BILLS-105s1146is.pdf, zuletzt besucht am 24.04.2016, zit.: S. 1146.

S. REP. 105-190, 105TH Cong., 2ND Sess. 1998, 1998 WL 239623 (Leg.Hist.) P.L. 105-304, THE DIGITAL MILLENNIUM COPYRIGHT ACT OF 1998, abrufbar unter https://www.congress.gov/105/crpt/srpt190/CRPT-105srpt190.pdf, zuletzt besucht am 24.04.2016, zit.: S. Rep. 105-190.

Stoltz: Victory for Open WiFi: Judge Rejects Copyright Troll's Bogus „Negligence" Theory, 11. Juli 2012, abrufbar unter https://www.eff.org/deeplinks/2012/07/judge-copyright-troll-cant-bully-internet-subscriber-bogus-legal-theory, zuletzt besucht am 28. August 2016, zit.: Stoltz: Victory for Open WiFi: Judge Rejects Copyright Troll's Bogus „Negligence" Theory.

Sullivan: The Yahoo Directory – Once The Internet's Most Important Search Engine – Is To Close, 26. September 2014, abrufbar unter http://searchengineland.com/yahoo-directory-close-204370, zuletzt besucht am 24.04.2016, zit.: Sullivan, The Yahoo Directory Is To Close.

Sydnor: In the Megaupload extradition, Professor Lessig shows what he knows – and doesn't know – about US copyright laws, 28. September 2015, abrufbar unter http://www.techpolicydaily.com/technology/megaupload-lessig/, zuletzt besucht am 24.04.2016, zit.: Sydnor.

Szpunar: Schlussanträge vom 16. März 2016, Rechtssache C-484/14 - Tobias Mc Fadden gegen Sony Music Entertainment Germany GmbH, abrufbar unter http://curia.europa.eu/juris/document/document.jsf?text=&docid=175130&pageIndex=0&doclang=DE&mode=req&dir=&occ=first&part=1, zuletzt besucht am 24.04.2016, zit.: Szpunar, Schlussanträge vom 16. März 2016.

Urban/Karaganis/Schofield: Notice and Takedown in Everyday Practice, 2016, abrufbar unter http://poseidon01.ssrn.com/delivery.php?ID=554072120067116098103076089081016098102019085079049016085026005127122011027099127018122122053012104056055089028067096126027083009086053083017027087065094123083107096005054011114079066111000005091009030119126017000003026094113026092104120111076001075097&EXT=pdf, zuletzt besucht am 24.04.2016, zit.: Notice and Takedown in Everday Practice.

Verband der deutschen Internetwirtschaft e.V. (eco): Stellungnahme zum Fragenkatalog des Bundesministeriums für Wirtschaft und Technologie zur Regelung der Anbieterhaftung im Telemediengesetz, abrufbar unter http://www.gesmat.bundesgerichtshof.de/gesetzesmaterialien/16_wp/elgvg/stellung_fragkat_eco.pdf, zuletzt besucht am 24.04.2016, zit.: eco, Stellungnahme zur Anbieterhaftung.

A. Einführung

I. Die Haftung der Internet Service Provider

Die wachsende Bedeutung von Wissen und Information und der damit einhergehende Wandel von der Industrie- zur Informationsgesellschaft hat auch die stetige Entwicklung neuer Informations- und Kommunikationstechnologien gefördert. Dabei hat das rasante Wachstum des Internets ab Mitte der neunziger Jahre viele neue Marktakteure hervorgebracht. Den Internet Service Providern[1] (ISP), welche eine Vielzahl unterschiedlicher Geschäftsmodelle betreiben, kommt insoweit eine maßgebliche Rolle zu.

Diese ISP lassen sich in fünf grundlegende Kategorien einordnen.[2] Der Access-Provider vermittelt seinen Nutzern Zugang zum Internet.[3] Der Cache-Provider übermittelt Informationen, meist zwischen Teilnetzen, und speichert diese in diesem Zusammenhang zur beschleunigten Übermittlung zeitlich begrenzt zwischen.[4] Der Host-Provider stellt Speicherplatz, bspw. in Form von öffentlichen Plattformen, für Inhalte Dritter bereit.[5] Die Suchmaschinenanbieter sowie sonstige Diensteanbieter, die Links auf fremede Webseiten bereithalten (Linksetzende), verlinken Inhalte zum erleichternden Auffinden von Informationen. Und der Content-Provider stellt eigene Inhalte zur Verfügung.[6]

Durch die verschiedenartigen ISP sind die Nutzer erst in der Lage, das Internet effizient zu nutzen. Und gerade diese Sachnähe zu den Nutzern ruft die ISP immer wieder auf den Plan, wenn es um Diskussionen bezüglich der Bekämpfung von Rechtsverletzungen im Internet geht. Die Verantwortlichkeit und

[1] Dt.: Internetdiensteanbieter.
[2] Hinsichtlich näherer Ausführungen zu den einzelnen ISP siehe S. 22.
[3] Sieber, Rn. 14.
[4] Sieber, Rn. 22.
[5] Sieber, Rn. 14.
[6] Sieber, Rn. 14.

Haftungsprivilegierung der ISP verlieren vor allem in der andauernden Urheberrechtsdebatte nicht an Aktualität und Brisanz.

Während der deutsche Gesetzgeber sich bereits 1997 mit dieser Thematik beschäftigte und in der Folge auf Bundesebene die ersten Haftungsprivilegien für ISP einführte, hat im Jahr 2000 auch der europäische Richtliniengeber seinen Mitgliedsstaaten die Einführung von Privilegien zur Umsetzung auferlegt. Ziel der gesetzlichen Festlegung von Privilegien war die Reduzierung und Eingrenzung der Gefahren für die verschiedenen Geschäftsmodelle sowie die Schaffung von Rechtssicherheit für die Anbieter. Dadurch wollte man innovative Geschäftsmodelle sowie den Wirtschaftsstandort Deutschland fördern[7] bzw. auf europäischer Ebene Rechtsunsicherheit jenseits der nationalen Grenzen beseitigen, um hierdurch das reibungslose Funktionieren des Binnenmarktes zu gewährleisten[8]. Aufgrund der verschiedenartigen Betätigungsfelder der Provider besteht eine abgestufte Verantwortlichkeit basierend auf der jeweiligen Nähe der ISP zum rechtswidrigen Inhalt. Diese den Haftungsprivilegien inhärente Differenzierung spiegelt somit die Möglichkeit zur Kontrolle und Einflussnahme der ISP auf die Inhalte wider.

Aber auch über 15 Jahre nach Einführung der Privilegien ist das Haftungsregime der ISP regelmäßig Mittelpunkt gerichtlicher Verfahren, sowohl auf nationaler als auch europäischer Ebene, sowie Gegenstand nationaler Gesetzgebungsinitiativen.

Zur Privilegierung der ISP wurden in den USA 1998 ebenfalls Haftungsbeschränkungen eingeführt.

Auch in den USA sind die Privilegien immer wieder Gegenstand des öffentlichen Diskurses. Derzeit ist eine Untersuchung zur Bewertung der Auswirkungen und der Effektivität des geltenden Haftungsregimes der ISP unter Federführung des U.S. Copyright Office anhängig.[9]

---

[7] Hoffmann in Spindler/Schuster, Vorbemerkung zu § 7 - § 10, Rn. 1.
[8] Vgl. auch Erwägungsgrund 40 der E-Commerce-Richtlinie.
[9] Siehe hierzu S. 357.

II. Problemstellung und Arbeitshypothese

Der Gesetzgeber stand bei der Entwicklung der Haftungsprivilegien für die ISP vor der Herausforderung, eine ausgewogene Balance zwischen den Interessen der im Internet aufeinandertreffenden Akteure sicherzustellen.

Die ISP sind in erster Linie an der Sicherung ihres Geschäftsmodells interessiert. Für ein reibungsloses Funktionieren sind sie auf rechtliche Rahmenbedingungen angewiesen, welche ihnen keine unverhältnismäßigen finanziellen und organisatorischen Bürden auferlegen.

Die Urheber und Rechteinhaber sind vorrangig an dem Schutz ihrer geistigen Eigentumsrechte interessiert. Von Bedeutung ist für sie auch eine einfache und effektive Rechtsdurchsetzung, welche u.a. dadurch sichergestellt wird, dass sie nicht nur gegen die unmittelbaren Verletzer, sondern auch gegen die im Internet auftretenden Intermediäre vorgehen können.

Die Nutzer sind heutzutage oftmals sog. „Prosumenten“[10] und damit zugleich auch Rechteinhaber, da sie Inhalte nicht mehr nur rein passiv konsumieren, sondern zugleich auch produzieren. Sie haben als passive Konsumenten ein vornehmliches Interesse an einer ungehinderten Informationsbeschaffung sowie am Schutz ihrer persönlichen Daten.

Das Spannungsverhältnis zwischen den unterschiedlichen verfassungsrechtlich geschützten Rechtsgütern, namentlich dem eingerichteten und ausgeübten Gewerbebetrieb der ISP, den Eigentumsrechten der Urheber sowie der Informationsfreiheit und dem Datenschutz der Internetnutzer, musste vom Gesetzgeber bei der Schaffung der Haftungsprivilegien beachtet werden.

Während den ISP durch die Einführung der Haftungsprivilegien eine Art Vertrauensvorschuss gewährt wurde, ging dies zu Lasten der Urheberrechtsinhaber, die hierdurch die ISP nur noch in eingeschränktem Umfang in Anspruch nehmen können. Dies ist insbesondere problematisch in Fällen in denen nur schwer an den

[10] Eine Verbindung der Begriffe „Produzent“ und „Konsument“.

tatsächlichen Rechtsverletzer heranzukommen ist oder in Fällen, in denen das Geschäftsmodell des ISP ganz offensichtlich auf die Förderung rechtswidriger Handlungen angelegt ist.

Im Jahr 2001 hat der europäische Richtliniengeber zwei weitere Richtlinien erlassen, die dem Schutz der Inhaber von Urheberrechten (InfoSoc-RL) oder sonstiger geistiger und gewerblicher Schutzrechte (Durchsetzungs-RL) dienen.[11] Obwohl Erwägungsgrund 16 der InfoSoc-RL klarstellt, dass die InfoSoc-RL nicht die Bestimmungen der ECRL zu Fragen der Haftung berührt, steht Art. 8 der InfoSoc-RL in einem Spannungsverhältnis zu den Haftungsprivilegien. Denn gem. Art. 8 Abs. 3 InfoSoc-RL sollen die Mitgliedsstaaten sicherstellen, dass die Rechteinhaber gerichtliche Anordnungen gegen Vermittler beantragen können, deren Dienste von einem Dritten zur Verletzung von Urheberrechten genutzt werden.[12] Der deutsche Gesetzgeber hat diese Bestimmung nicht in deutsches Recht umgesetzt, da er der Auffassung war, dass bereits nach geltendem Recht entsprechende Anordnungen gegen Vermittler beantragt werden können.

Ob der Gesetzgeber mit Schaffung der Haftungsprivilegien eine ausgewogene Rechtssituation geschaffen hat, wurde seitdem durch eine Vielzahl von Gerichtsentscheidungen bewertet.

Die Gerichte versuchen durch ihre Rechtsprechung laufend die gesetzlichen Regelungen zu konkretisieren und auszudifferenzieren, um so die widerstreitenden Interessen ins Gleichgewicht zu bringen. Ob ihnen dies gelungen ist, erscheint fraglich, denn durch eine die Privilegierung der ISP einschränkende Rechtsprechung wurden wiederum Unsicherheiten seitens der ISP geschürt, die der ursprünglichen Intention des Gesetzgebers, für solche ISP Rechtssicherheit zu schaffen, zuwiderlaufen.

Mit einer der ersten höchstrichterlichen Entscheidungen nach

---

[11] Richtlinie 2001/29/EG des Europäischen Parlaments und des Rates vom 22. Mai 2001 zur Harmonisierung bestimmter Aspekte des Urheberrechts und der verwandten Schutzrechte in der Informationsgesellschaft („InfoSoc-RL“) sowie Richtlinie 2004/48/EG des Europäischen Parlaments und des Rates vom 29. April 2004 zur Durchsetzung der Rechte des geistigen Eigentums („Durchsetzungs-RL“).

[12] Eine fast wortgleiche Regelung enthält Art. 11 S. 3 Durchsetzungs-RL.

Umsetzung der ECRL, hat der BGH ausgeführt, dass die Privilegien des Host-Providers grundsätzlich nicht auf negatorische Ansprüche anwendbar seien.[13] Dem Host-Provider werden vielmehr im Rahmen der Störerhaftung Prüfpflichten auferlegt, deren Verletzung eine Verantwortlichkeit begründet.

Dies bedeutet, dass der Host-Provider, nachdem er Kenntnis von einer bestimmten Rechtsverletzung erlangt hat, diese unverzüglich zu entfernen und darüber hinaus dafür Sorge zu tragen hat, dass es nicht zu weiteren kerngleichen Rechtsverletzungen kommt. Dies gilt nach einem zweiten Urteil des gleichen Senats auch für vorbeugende Unterlassungsansprüche.[14] Der Host-Provider hafte als Störer, sofern eine entsprechende Erstbegehungsgefahr begründet sei.[15]

Zudem sieht der BGH nicht nur eine Verantwortlichkeit des Host-Providers für eigene Informationen, sondern zugleich für sog. „zu eigen gemachte" Informationen.[16] Dies sind Informationen, die ursprünglich von einem Dritten stammen, die der Host-Provider sich jedoch durch gewisse Handlungen als eigene zurechen lassen muss.

In zwei BGH-Entscheidungen aus dem Jahr 2014 wendet der Gerichtshof die für den Host-Provider aufgestellten Grundsätze der Unanwendbarkeit der Privilegien auf negatorische Ansprüche auch auf den Access-Provider an und legt diesem Prüfpflichten nach Kenntnis einer konkreten Rechtsverletzung auf.[17]

Im Hinblick auf den Host-Provider wurde die frühe Rechtsprechung hinsichtlich einer generellen Unanwendbarkeit auf Unterlassungsansprüche jedoch durch die „L'Oréal"-Entscheidung des EuGH[18] im Jahr 2011 und die darauf folgenden Entscheidungen des BGH[19] in Zweifel gezogen. Auch wenn weder der EuGH noch der BGH ausdrücklich auf die bisherige Rechtsprechung des BGH

[13] BGHZ 158, 236 = BGH MMR 2004, 668 – „Internetversteigerung I".
[14] BGHZ 172, 119 = MMR 2007, 507 – „Internetversteigerung II".
[15] BGH GRUR 2007, 708, 711.
[16] BGH MMR 2010, 556 – „marions-kochbuch.de.
[17] Hierzu ausführlich S. 107 und S. 159.
[18] EuGH, MMR 2011, 596 – „L'Oréal SA".
[19] BGH GRUR 2016, 268 – „Goldesel"; BGH MMR 2016, 188 – „3dl.am".

hinsichtlich einer Unanwendbarkeit der Haftungsprivilegien auf Unterlassungsansprüche Bezug genommen haben, so wertet ein Teil des Schrifttums die an das EuGH-Urteil anschließende Rechtsprechung des BGH als zumindest teilweise Abkehr seiner bisherigen Leitlinie.[20]

Folge dieser Rechtsprechung ist die sowohl im Schrifttum als auch in der Rechtsprechung herrschende Uneinigkeit über die grundsätzliche Unanwendbarkeit auf Unterlassungsansprüche und Ungewissheit hinsichtlich des genauen Umfangs der dem ISP aufzuerlegenden Prüfpflichten.

Diese Arbeit untersucht, inwieweit die Rechtsprechung den Zielen des Gesetzgebers bei der Einführung der Privilegien Rechnung getragen hat und eine ausgewogene Balance zwischen den verschiedenen Interessen der involvierten Akteure hergestellt hat.

Ihr liegt die Hypothese zugrunde, dass durch die Ausweitung der Verantwortlichkeit der ISP durch die Rechtsprechung die gesetzlich stipulierte Haftungsprivilegierung faktisch entwertet wird. Insbesondere stehen die Nichtanwendung der Privilegien auf Unterlassungsansprüche sowie die im Rahmen der Störerhaftung begründeten Prüfpflichten der Intention des Gesetzgebers (auch auf europäischer Ebene) entgegen.

Eine gerechte Balance der Interessen der Akteure durch die Rechtsprechung wurde nicht erreicht.

Die gesetzliche Ausgestaltung der US-amerikanischen Privilegierung verspricht hingegen eine den Interessen der ISP gerechtere Lösung. Auch die Rechtsanwendung der US-amerikanischen Gerichte liegt hiermit auf einer Linie.

III. Methodik der Untersuchung

Die dieser Arbeit zugrunde liegende Hypothese wird anhand eines Rechtsvergleichs in Form des Mikrovergleichs[21] untersucht. Als Vergleichsland zu Deutschland dienen die USA. Diese verfügen

[20] So insbesondere KG Berlin ZUM 2013, 886, 889. Vgl. hierzu S. 76.

[21] Siehe hierzu Haase, JA 2005, 232, 236. Der Mikrovergleich ist auf klar abgrenzbare Details einer bestimmten Rechtsordnung beschränkt und beleuchtet einzelne, spezielle Rechtsfragen.

über in weiten Teilen übereinstimmende gesetzliche Regelungen hinsichtlich der Privilegierung der ISP, welche jedoch an verschiedenen Stellen teils signifikante Abweichungen zur deutschen bzw. europäischen Lösung aufweisen. Abgesehen von den gesetzlich begründeten Unterschieden liegt die wohl größte Divergenz in der Rechtsanwendung der gesetzlichen Bestimmungen.

Die USA eignen sich besonders aufgrund ihres Rufs als „Start-up-Mekka“ als Vergleichsland, welches insbesondere im Bereich Technologie und Internet mit Silicon Valley als Flaggschiff alteingesessene Giganten wie Google, Apple, facebook und eBay sowie Aufsteiger wie Uber, Netflix und Airbnb beherbergt. Obwohl sowohl die USA als auch Deutschland zu den innovativsten Industriestaaten der Welt zählen, nehmen die USA im Wirtschaftsbereich gegenüber Deutschland eine Führung ein.[22] Ein Grund hierfür könnte im Vorsprung der USA im Bereich der revolutionären Innovation liegen, wohingegen Deutschland eher im Bereich der evolutionären Innovation punkten kann.[23]

Für eine innovationsfreundliche Gesellschaft sind gerade die Schaffung sicherer rechtlicher Rahmenbedingungen und der Abbau von Investitionshindernissen unabdingbar. Hierzu kann neben der gesetzgeberischen Initiative auch der Rechtsprechung eine gewichtige Rolle zukommen.

IV. Stand der Forschung

In der Literatur bietet die Verantwortlichkeit der ISP und die Begrenzung ihrer Haftungsprivilegien durch die Gerichte immer wieder Anlass für eine rege Diskussion.

---

[22] Die USA landen im Innovationsindikator 2015 mit 58 Punkten auf Rang 3 während Deutschland mit 56 Punkten Rang 6 für sich beanspruchen kann. Einzelne Ländervergleiche sind individuell abrufbar unter http://www.innovationsindikator.de/mein-indikator/, zuletzt besucht am 23.04.2016.

[23] Start-ups in Deutschland und den USA, S. 3. Eine evolutionäre Innovation bezeichnet die Verbesserung eines bestehenden Produktes während die revolutionäre Innovation die Schaffung und Erschließung von neuen Produkten und Märkten bezeichnet.

Während die wohl h.M. in der Literatur noch immer davon ausgeht, dass die Privilegien nach der Rechtsprechung des BGH weiterhin nicht auf Unterlassungsansprüche anwendbar sind[24], werden die Folgen dessen recht unterschiedlich bewertet.

Nolte und *Wimmers* sind der Auffassung, dass das Ziel der Schaffung von Rechtssicherheit nicht erreicht wurde und der I. Zivilsenat mit der Störerhaftung ein von den Privilegien des TMG losgelöstes Haftungssystem entwickelt hat.[25] Als Lösung schlagen sie eine grundsätzliche Subsidiarität der ISP-Haftung vor, zusammen mit einer Änderung der ZPO, die eine gerichtliche Anordnung gegen Unbekannt ermöglicht, so dass Rechteinhaber in erster Linie gegen die tatsächlichen Rechtsverletzer vorgehen können und nicht gegen die lediglich mittelbar beteiligten ISP.[26] Zudem plädieren Sie hinsichtlich des Host-Providers für die Einführung eines *Notice and Takedown*-Verfahrens nach amerikanischem Vorbild mit dem zusätzlichen Erfordernis der Glaubhaftmachung einer Rechtsverletzung.[27]

Auch *Hoeren*, der grundsätzlich der Auffassung ist, dass auch Unterlassungsansprüche unter die Privilegien fallen, geht davon aus, dass im Hinblick auf den Host-Provider durch die weite Ausdehnung des Unterlassungsanspruches auch auf zukünftige kerngleiche Rechtsverletzungen die Zielrichtung des TMG sowie der ECRL außer Acht gelassen wurde und dies zur Rechtsunsicherheit der ISP beigetragen hat.[28] Folge dessen sei eine Interessenabwägung im Einzelfall, welche gerade durch die Schaffung der Privilegien vermieden werden sollte. Er plädiert daher für eine Verpflichtung des Host-Providers, lediglich einen konkret abgemahnten Inhalt zu entfernen, so wie es auch dem

[24] Vgl. u.a. Krüger/Apfel, MMR 2012, 144, 145; Fitzner, GRURInt 2012, 109, 144; Hoffmann in Spindler/Schuster, § 10 TMG Rn. 3; Sieber/Höfinger in Hoeren/Sieber/Holznagel, Teil 18.1, Rn. 50; Nordemann, GRUR 2011, 977; jedenfalls für Host-Provider: Müller-Broich, § 10 Rn. 1.
[25] Nolte/Wimmers, GRUR-Beilage 2014, 58 ff.
[26] Nolte/Wimmers, GRUR-Beilage 2014, 58, 68 f.
[27] Nolte/Wimmers, GRUR-Beilage 2014, 58, 69.
[28] Hoeren in Festschrift für Ulrich Eisenhardt, S. 243, 253.

Wortlaut des § 7 Abs. 2 S. 2 TMG entspricht.[29] Den Host-Provider würde hierdurch nur eine Beseitigungspflicht treffen. Kommt er dieser Verpflichtung nach, ist er im Sinne des TMG auch hinsichtlich Unterlassungsansprüchen privilegiert.[30]

Spindler hingegen vertritt die Auffassung, dass das vom BGH entwickelte Konzept der Störerhaftung des Host-Providers durch den EuGH bekräftigt wurde, jedoch die erforderliche Einzelfallabwägung zwischen dem Verbot allgemeiner Überwachungspflichten und spezifischer Schutzmaßnahmen zu Rechtsunsicherheit führt.[31] Hinsichtlich des Access-Providers sieht er aufgrund europäischer Rechtsprechung eine unmittelbare Anwendbarkeit der Privilegien auf die Unterlassungspflichten aus der Störerhaftung nicht geboten, attestiert aber auch hier eine zunehmende Rechtsunsicherheit aufgrund der vom Access-Provider geforderten Interessenabwägung im Einzelfall.[32]

Dahingegen ist *Leistner* der Auffassung, der BGH habe mit seiner Rechtsprechung ein grundsätzlich ausgewogenes System geschaffen.[33] Insbesondere seien die Voraussetzungen der Störerhaftung durch zahlreiche Entscheidungen konkretisiert worden, welche auch dem wirtschaftlichen Interesse der ISP Rechnung tragen würden.[34] Auch das Konstrukt des BGH hinsichtlich „zu eigen gemachter" Inhalte befürwortet er vor dem Hintergrund einer, bspw. durch die redaktionelle Gestaltung der Inhalte, erlangten Kontrolle.[35]

Leistner und *Grisse* sehen zudem nach der Rechtsprechung des EuGH eine Unanwendbarkeit der Privilegien auf Unterlassungsansprüche für sämtliche ISP als geboten an.[36]

Die gesetzlichen Regelungen und die hierauf basierende Rechtsprechung der ISP-Haftung in den USA wurden bereits des

[29] Hoeren in Festschrift für Ulrich Eisenhardt, S. 243, 252.
[30] Hoeren in Festschrift für Ulrich Eisenhardt, S. 243, 252.
[31] Spindler, MMR 2011, 703, 706 f.
[32] Spindler, GRUR 2014, 826, 834.
[33] Leistner, ZUM 2012, 722.
[34] Leistner, ZUM 2012, 722, 724.
[35] Leistner, ZUM 2012, 722, 732.
[36] Leistner/Grisse, GRUR 2015, 19, 21.

Öfteren im Schrifttum als Vergleich zu Deutschland herangezogen, zumeist jedoch beschränkt auf den Host-Provider.[37] Insbesondere das *Notice and Takedown*-Verfahren des US-amerikanischen Rechts wird immer wieder als Paradebeispiel angebracht, wenn es darum geht, dem Host-Provider mehr Rechtssicherheit zu verschaffen.[38] *Holznagel* widmete seine Dissertation dem US-amerikanischen *Notice and Takedown*-Verfahren als Teil der Providerhaftung.[39] Er beschränkt sich hierbei jedoch auf den Host-Provider, untersucht insoweit hauptsächlich die einzelnen Merkmale des US-amerikanischen Systems und versucht anschließend die einzelnen Elemente des *Notice and Takedown*-Verfahrens im deutschen Recht zu verorten. Als Ergebnis präsentiert er eine *Notice and Takedown*-Regelung, in Anlehnung an das US-amerikanische Recht. Mit der Nichtanwendung der Privilegien auf Unterlassungsansprüche im deutschen Recht beschäftigt er sich nur am Rande.

Eine alle ISP einbeziehende, rechtsvergleichende, analytische und monografische Untersuchung, die der Frage nachgeht, ob das von Gesetzgeber und Rechtsprechung geschaffene Konzept der ISP-Haftung den nationalen und europäischen Zielen gerecht wird und ob aus der US-amerikanischen Lösung Ansätze für eine interessengerechtere nationale Gestaltung hergeleitet werden können, existiert bislang nicht.

V. Gang der Untersuchung

Zunächst werden im ersten Teil die technischen und begrifflichen Grundlagen vermittelt, die für eine weitere Lektüre dieser Arbeit notwendig sind.

Der darauffolgende Teil behandelt die Verantwortlichkeit und Privilegien der verschiedenen ISP in Deutschland. Dort werden die anhand der Rechtsprechung herausgebildeten, aktuellen

[37] Fitzner, GRUR Int 2012, 109; Holznagel, GRUR Int 2014, 105; Holznagel, GRUR Int 2010, 654; Ott, GRUR Int 2008, 563; Spindler/Leistner, GRUR Int 2005, 773.

[38] So auch Fitzner, GRUR Int 2012, 109, 116; Holznagel, GRUR Int 2014, 105, 113; Ott, GRUR Int 2008, 563;

[39] Holnagel, Notice and Take-Down-Verfahren als Teil der Providerhaftung.

Problemfelder in Deutschland dargestellt und deren Auswirkungen untersucht. Hauptaugenmerk liegt hier auf dem Host-Provider, um den es zumeist auch im öffentlichen Diskurs geht und welcher den Inhalten seiner Nutzer am nächsten steht. Zudem wird die Verantwortlichkeit des Cache- und Access-Providers sowie sonstiger ISP in Deutschland unter Bezugnahme auf die aktuelle Rechtsprechung und bestehende Gesetzgebungsinitiativen beleuchtet.

In einem dritten Teil wird die Verantwortlichkeit und Privilegierung der ISP in den USA behandelt. Auch hier wird im Aufbau zwischen Host-, Cache- und Access-Provider sowie sonstigen ISP differenziert. Unter Bezugnahme auf die gesetzlichen Bestimmungen sowie einer Analyse des hierauf aufbauenden Richterrechts wird die Rolle der ISP im US-amerikanischen Recht untersucht.

Der vierte Teil der Arbeit befasst sich mit dem Ländervergleich. Er bewertet unter Bezugnahme der Ergebnisse des Ländervergleichs des zweiten und dritten Teils den deutschen Kurs. Der letzte Teil enthält die Verifizierung der Arbeitshypothese und zeigt auf dem Rechtsvergleich aufbauende Lösungsvorschläge auf.

B. Technische und begriffliche Grundlagen

Da die Verantwortlichkeit der ISP an deren inhaltliche Nähe zum rechtswidrigen Inhalt anknüpft und auch die zu ergreifenden Maßnahmen und Pflichten sich daran bemessen, was dem ISP technisch überhaupt möglich und zumutbar ist, werden im Folgenden zunächst die technischen Grundlagen des Internets sowie die für eine Beurteilung der jeweiligen Rolle der ISP notwendigen Informationen zur Funktionsweise der unterschiedlichen Dienste der ISP dargestellt.

Auf eine Darstellung der Geschichte des Internets wird aufgrund der bereits vielfach an anderer Stelle ausführlichen Abhandlungen[40] verzichtet. Die nachfolgende Skizzierung soll lediglich rudimentäre

[40] Vgl. bspw. Sieber in Hoeren/Sieber/Holznagel, Teil 1, Rn. 1 ff. m.w.N.

technische Kenntnisse hinsichtlich der Funktionsweise des Internets sowie begriffliche Grundlagen im Hinblick auf die unterschiedlichen Internetdienste vermitteln, welche für die darauffolgenden Ausführungen in Bezug auf die ISP sinnvoll erscheinen.

I. Das Internet

Der Begriff des Internets bezeichnet ein weltweites Computernetzwerk, welches auf einem vereinheitlichten Übertragungsprotokoll (TCP/IP[41]) basiert. Dieses dient der Übertragung unterschiedlicher Daten zwischen verschiedenen Computern. Je nach Rolle des jeweiligen Computers wird zwischen „Client“ und „Server“ unterschieden. Client ist, wer bestimmte Daten abfragt, welche ihm der Server dann zur Verfügung stellt.[42]

Die Kommunikation der Computer untereinander im Sinne eines Austauschs von Daten geschieht nach Digitalisierung der Daten durch Umwandlung in Binärcodes. Die kleinste Einheit bildet ein „Bit“. Um die auf diese Weise umgewandelten Daten im Netzwerk von einem Computersystem zu einem anderen Computersystem zu übertragen, werden den beteiligten Computern jeweils IP-Adressen zugeteilt. Durch die Zuweisung einer IP-Adresse sind die Computersysteme im Netzwerk überhaupt erst adressierbar und damit auch erreichbar.

Es wird zwischen statischen und dynamischen IP-Adressen unterschieden. Statische Adressen sind fest an einen Computer oder Server vergeben, während dynamische IP-Adressen erst bei Bedarf dem jeweiligen Computer zugewiesen werden.[43] Statische IP-Adressen sind beispielsweise erforderlich für den Betrieb eigener Server, beispielsweise einem Webserver[44] oder Mailserver[45], damit diese für den Nutzer immer eindeutig erreichbar sind.

---

[41] Akronym für Transmission Control Protocol/Internet Protocol.
[42] Sieber in Hoeren/Sieber/Holznagel, Teil 1, Rn. 20.
[43] Schmitz in Hoeren/Sieber/Holznagel, Teil 16.2, Rn. 108 ff.
[44] Das sind Computersysteme, die Webseiten anbieten, siehe hierzu auch Sieber in Hoeren/Sieber/Holznagel, Teil 1, Rn. 48.
[45] Dieser ist notwendig zur Nutzung eines E-Mail-Dienstes, siehe hierzu auch Sieber in Hoeren/Sieber/Holznagel, Teil 1, Rn. 113 ff.

Da die aus Zahlen bestehende IP-Adresse sich nur schwer einprägen lässt, wird dieser im Falle einer Webseite ein eindeutiger Name zugeordnet, der sog. Internet Domain Name. Die Zuordnung erfolgt durch das Domain Name System (DNS). Bei einer durch die Verwendung des Domainnamens gestarteten Nutzeranfrage, ermittelt der Name Server die hierzu korrespondierende IP-Adresse und stellt entsprechend die Verbindung her.[46]

Im Internet gibt es unterschiedliche Dienste, wie beispielsweise das World Wide Web, E-Mail, das Usenet und File Transfer Protocol.[47] Im Folgenden werden lediglich die Dienste und Anwendungsprotokolle aufgeführt, welche für die weitere Abhandlung von Bedeutung sind.

1. World Wide Web

Wenn im allgemeinen Sprachgebrauch die Rede von dem Internet[48] ist, wird hiermit meist das World Wide Web (WWW) bezeichnet. Dieses stellt eine Anwendung innerhalb des Internets dar. Es basiert auf dem Hypertext Transfer Protocol (HTTP) und besteht aus einer Vielzahl von Hypertext-Systemen, sog. Webseiten, welche durch Hyperlinks miteinander verknüpft sind.[49] Der Nutzer kann diese Webseiten mittels eines Browsers aufrufen, welcher für die grafische Darstellung der Webseiten sorgt. Beispiele hierfür sind der Microsoft Internet Explorer[50] oder Mozilla Firefox[51]. Durch die Eingabe einer sog. URL[52] erfolgt die Adressierung einer bestimmten Datei im WWW.

Während das WWW lange Zeit hauptsächlich zum Abruf von Dokumenten genutzt wurde, enthalten Webseiten heute oftmals eine starke interaktive Komponente.[53] Beispiele hierfür sind Gästebücher, Diskussionsforen, Wikis oder Blogs, welche es dem

---

[46] Sieber in Hoeren/Sieber/Holznagel, Teil 1, Rn. 59.
[47] Sieber in Hoeren/Sieber/Holznagel, Teil 1, Rn. 79.
[48] Kurz für „Interconnected Networks“.
[49] Sieber in Hoeren/Sieber/Holznagel, Teil 1, Rn. 80.
[50] Siehe http://www.microsoft.com/de-de/download/internet-explorer.aspx, zuletzt besucht am 23.04.2016..
[51] Siehe https://www.mozilla.org/de/firefox/new/, zuletzt besucht am 23.04.2016.
[52] Akronym von Uniform Resource Locator.
[53] Sieber in Hoeren/Sieber/Holznagel, Teil 1, Rn. 91.

Nutzer ermöglichen, eigene Inhalte unterschiedlichster Art auf der jeweiligen Webseite zu platzieren.[54]

2. File Transfer Protocol

Das File Transfer Protokol (FTP) ermöglicht die Übertragung von Dateien zwischen zwei Computern im Internet.[55] Dateien können entweder vom FTP-Server zum Client (sog. Download) oder vom Client zum FTP-Server (sog. Upload) übertragen werden.[56]
Zugang zu einem FTP-Server enthält der Nutzer entweder in dem er sich ein eigenes Benutzerkonto anlegt oder der FTP-Betreiber gestattet den freien Datenabruf, also ohne vorherige Anmeldung.[57]

3. Proxy-Server

Bei dem Proxy-Server[58] handelt es sich um einen Vermittler- bzw. Weiterleiter-Dienst auf einem Rechnerknoten zwischen Client und Server.[59] Da er sowohl Anfragen des Client entgegennimmt und an den Server im Namen des Client weiterleitet als auch die Antwort des Servers empfängt und in dessen Namen an den Client weiterleitet, verhält er sich gegenüber dem Client wie ein Server und gegenüber dem Server wie ein Client.[60]
Der Proxy-Server kann zudem durchgeleitete Inhalte zwischenspeichern, um diese auf erneute Anfrage eines anderen Client schneller direkt aus dem Cache ohne erneute Interaktion mit dem Server weiterzuleiten.[61]

4. Usenet

Das Usenet[62] ist ein weltweites Netzwerk, welches aus einer Vielzahl fachlicher Diskussionsforen, sog. Newsgroups, besteht. In

---

[54] Ausführlich hierzu Sieber in Hoeren/Sieber/Holznagel, Teil 1, Rn. 91 ff.
[55] Sieber in Hoeren/Sieber/Holznagel, Teil 1, Rn. 131.
[56] Sieber in Hoeren/Sieber/Holznagel, Teil 1, Rn. 131.
[57] Sieber in Hoeren/Sieber/Holznagel, Teil 1, Rn. 132.
[58] Vom englischen Begriff „Proxy“ = Stellvertreter.
[59] Pfitzmann/Köpsell/Kriegelstein, Sperrverfügungen gegen Access-Provider, S. 20.
[60] Pfitzmann/Köpsell/Kriegelstein, Sperrverfügungen gegen Access-Provider, S. 20.
[61] Pfitzmann/Köpsell/Kriegelstein, Sperrverfügungen gegen Access-Provider, S. 26. Er wird deshalb auch oft als Proxy-Cache Server bezeichnet, siehe hierzu S. 24.
[62] Abkürzung für Unix User Network.

seiner Funktion wird es oftmals mit dem analogen schwarzen Brett verglichen, da jeder Nutzer eine Nachricht an eine von ihm gewählte Newsgroup senden kann und diese dort „gepostet“, also quasi an das schwarze Brett gepinnt wird, und damit für die anderen Nutzer einsehbar ist.[63] Im Unterschied zur analogen Variante können die anderen Nutzer der Newsgroup auf diese Nachricht allerdings unmittelbar antworten bzw. diese kommentieren. Um Zugang zum Usenet zu erhalten, benötigt der Nutzer lediglich ein auf seinem Rechner installiertes Programm, den sog. Newsreader.[64]

Während in den meisten Newsgroups lediglich das Posten von Textdateien möglich ist, können in dem Binary-Usenet überdies Dateianhänge, sog. Binärdaten, gepostet werden.[65] Im allgemeinen Sprachgebrauch wird dies allerdings auch lediglich als Usenet bezeichnet.

Zum Betrieb des Usenets sind sog. Newsserver erforderlich, welche die Dateien ihrer Nutzer sowohl speichern als auch an die anderen Newsserver übermitteln.[66] Theoretisch ist hierfür jeder PC geeignet.[67] Es gibt folglich keinen zentralen Administrator, die gesamten Dateien sind vielmehr dezentral auf mehreren Tausend Newsservern gespeichert.

5. Peer-to-Peer

Bei sog. Peer-to-Peer-Netzwerken[68] handelt es sich um Filesharing-Systeme, bei denen die Nutzer unmittelbar untereinander Dateien austauschen können.[69] Der größte Unterschied zum Client-Server-Modell ist, dass hier jeder Computer sowohl als Client als auch als Server fungiert, wodurch ein dezentrales Datenverteilsystem entsteht, in dem jeder Computer gleichberechtigt ist und die

[63] Sieber in Hoeren/Sieber/Holznagel, Teil 1, Rn. 146.
[64] Sieber, Rn. 54.
[65] Bosbach/Wiege, ZUM 2012, 293, 294.
[66] Sieber in Hoeren/Sieber/Holznagel, Teil 1, Rn. 149.
[67] Sieber in Hoeren/Sieber/Holznagel, Teil 1, Rn. 149.
[68] Vom englischen „peer“ = Ebengebürtige(r)/Gleichgestellte(r), im allgemeinen Sprachgebrauch auch P2P-Netzwerk genannt.
[69] Sieber in Hoeren/Sieber/Holznagel, Teil 1, Rn. 139.

gleichen Dienste ausführt.[70] Die Dateien befinden sich also nicht mehr auf einem Server, sondern die Computer sind innerhalb des Netzwerkes direkt miteinander verbunden und die Dateien befinden sich folglich auf einer Vielzahl von Computern, sog. Peers.[71]

Es gibt allerdings Peer-to-Peer-Technologien, bei denen die Lokalisierung einer bestimmten abgerufenen Datei über einen zentralen Server läuft, der dann wie ein Verzeichnis bezüglich der im Netzwerk zu findenden Daten fungiert.[72] Auf Anfrage eines Nutzers innerhalb des Netzwerkes teilt der zentrale Server dem Anfragenden mit, wo sich die Datei befindet.[73] Die Verbindung zum Austausch der Datei erfolgt dann allerdings wieder direkt zwischen den zwei Computern.[74]

6. Hyperlinks und Deep-Links

Als Hyperlink bezeichnet man eine Verweisung auf einer Webseite auf eine andere Webseite, meist durch grafisch hervorgehobene Felder oder Wörter.[75] Klickt der Nutzer auf einen Hyperlink, so wird der mit dem Hyperlink verbundene Inhalt abgerufen, d.h. der Nutzer wird auf die entsprechende Webseite mit dem Inhalt geleitet.[76] Eine Art von Hyperlinks sind sog. Deep-Links, welche nicht auf die Homepage, also die Startseite einer Webseite, einer bestimmten Webseite verweisen, sondern auf Inhalte unterhalb der Homepage.[77]

7. Framing/In-line Linking

Beim Framing oder In-line Linking handelt es sich um eine besondere Form des Verlinkens von Inhalten. Anders als bei Hyperlinks werden nicht lediglich Verweisungen auf Inhalte Dritter gesetzt, sondern die Inhalte werden unmittelbar auf der Webseite des Verlinkenden eingebettet und dort bei Aufruf der

[70] Sieber in Hoeren/Sieber/Holznagel, Teil 1, Rn. 139 f.
[71] Sieber in Hoeren/Sieber/Holznagel, Teil 1, Rn. 139.
[72] Sieber in Hoeren/Sieber/Holznagel, Teil 1, Rn. 140.
[73] Sieber in Hoeren/Sieber/Holznagel, Teil 1, Rn. 140.
[74] Sieber in Hoeren/Sieber/Holznagel, Teil 1, Rn. 140.
[75] Boemke in Hoeren/Sieber/Holznagel, Teil 11, Rn. 67.
[76] Sieber, Rn. 64.
[77] Boemke in Hoeren/Sieber/Holznagel, Teil 11, Rn. 71.

entsprechenden Seite automatisch dargestellt, ohne dass es einer zusätzlichen Handlung des Nutzers bedarf.[78] Dadurch ist für den Nutzer nicht notwendigerweise erkennbar, dass die Inhalte ursprünglicherweise von einer anderen dritten Webseite stammen und es kann der Eindruck entstehen, dass es sich um Inhalte der verlinkenden Webseite handelt.[79]

8. Netzsperren

Die Thematik der Netzsperren findet regelmäßig Einzug in den politischen Diskurs, sei es in Form des Gesetzes zur Erschwerung des Zugangs zu kinderpornographischen Inhalten in Kommunikationsnetzen, einer Änderung des Glücksspielstaatsvertrages hinsichtlich unerlaubter Glücksspielangebote oder in Form von gerichtlichen Sperrverfügungen gegen Access-Provider.[80]

Um die andauernden Diskussionen bezüglich solcher Sperren nachvollziehen zu können, ist es notwendig, die drei zur Verfügung stehenden Sperren von der technischen Funktionsweise her zu verstehen.

a) DNS-Sperre

Wie unter Ziffer I ausgeführt, dient der DNS dazu, der IP-Adresse einen eindeutigen Domainnamen zuzuordnen. Wird nun eine DNS-Sperre eingesetzt, so bewirkt diese, dass bei Eingabe eines bestimmten Domainnamens eine fehlerhafte IP-Adresse zugeordnet wird und dadurch die Verbindung fehlschlägt.[81] Die Kommunikation mit dem DNS-Server wird dadurch verhindert.

b) IP-Sperre

Nutzt man zur Sperrung eine IP-Sperre, so bewirkt diese, dass auf sämtliche unter einer IP-Adresse erreichbare Inhalte nicht mehr zugegriffen werden kann. Da eine IP-Adresse mehrere Domains

---

[78] Micklitz/Namyslowska in Spindler/Schuster, § 5 UWG, Rn. 134.
[79] So auch Micklitz/Namyslowska in Spindler/Schuster, § 5 UWG, Rn. 134.
[80] Frey/Rudolph/Oster, MMR-Beilage 2012, 1, 1.
[81] Pfitzmann/Köpsell/Kriegelstein, Sperrverfügungen gegen Access-Provider, S. 52.

hosten kann, kann die IP-Sperre zu dem Ergebnis führen, dass alle unter der IP-Adresse zu erreichenden Domains, also auch zulässige Angebote, gesperrt werden.[82]

c) URL-Sperre

Bei der URL-Sperre wird durch den Einsatz eines Zwangs-Proxys die URL als genaues Zuordnungskriterium einer bestimmten Website gesperrt.[83] Hierbei wird der Datenverkehr des Nutzes automatisch über den Proxy geleitet und Anfragen auf unzulässige Inhalte gefiltert und der Zugriff hierauf verweigert oder auf eine vordefinierte Seite im Browser umgeleitet.[84]

II. Telemedien

Der Begriff der Telemedien ist in § 1 Abs. 1 S. 1 TMG definiert und umfasst danach alle elektronischen Informations- und Kommunikationsdienste, soweit sie nicht Telekommunikationsdienste nach § 3 Nr. 24 des Telekommunikationsgesetzes (TKG), die ganz in der Übertragung von Signalen über Telekommunikationsdienste bestehen, telekommunikationsgestützte Dienste nach § 3 Nr. 25 TKG oder Rundfunk nach § 2 des Rundfunkstaatsvertrages (RStV) sind.

1. Positives Abgrenzungsmerkmal

Einziges positives Abgrenzungsmerkmal ist damit der „elektronische Informations- und Kommunikationsdienst“. Unter diesen Begriff fallen sowohl Telemedien als auch Telekommunikationsdienste und Rundfunk. Eine Definition des Begriffs enthält weder das TMG, noch das TKG oder der RStV, er setzt sich jedoch aus drei unterschiedlichen Merkmalen zusammen.

[82] Pfitzmann/Köpsell/Kriegelstein, Sperrverfügungen gegen Access-Provider, S. 54 f.
[83] Pfitzmann/Köpsell/Kriegelstein, Sperrverfügungen gegen Access-Provider, S. 52.
[84] Pfitzmann/Köpsell/Kriegelstein, Sperrverfügungen gegen Access-Provider, S. 52.

a) Dienst

Bezeichnet im Einklang mit Art. 1 Nr. 2 der Informationsrichtlinie[85] eine Dienstleistung. Der Anwendungsbereich ist damit begrenzt auf ein Anbieter-Nutzer-Verhältnis. Ein Nutzer-Nutzer-Verhältnis, wie beispielsweise bei der Individualkommunikation zwischen zwei Nutzern, fällt aus der Begriffsdefinition heraus.[86]

b) Elektronisch

Der Dienst muss elektronisch erbracht werden, was insbesondere das Internet erfasst.[87] Denkbar sind jegliche Arten multimedialer Angebote, die unter die Kategorien Rundfunk, Telemedien und Telekommunikationsdienste fallen.[88] Im Bereich der Telemedien hat nicht nur die der Telekommunikation zugerechnete Übertragung elektronisch zu erfolgen hat, sondern auch die Bereitstellung der Inhalte.[89]

c) Information und Kommunikation

Gegenstand des elektronischen Dienstes muss Information bzw. Kommunikation sein. Diese kann sowohl in Bild-, Text- oder Tonform bereitgestellt werden.[90] Die Begriffe der Information und Kommunikation sind dabei denkbar weit zu fassen und umfassen sowohl das Online-Angebot von Waren und Dienstleistungen mit unmittelbarer Bestellmöglichkeit als auch die Versendung von Werbe-E-Mails.[91]

2. Negative Abgrenzungsmerkmale

Die Definition der Telemedien beruht damit größtenteils auf einer Negativabgrenzung zu den drei Diensten des TKG und RStV. Folglich ist für die Bestimmung des Begriffs des Telemediums eine

[85] Richtlinie 98/34/EG des Europäischen Parlaments und des Rates vom 22. Juni 1998 über ein Informationsverfahren auf dem Gebiet der Normen und technischen Vorschriften und der Vorschriften für die Dienste der Informationsgesellschaft.
[86] Altenhain in MüKo zum StGB, § 1 TMG, Rn. 9.
[87] Martini in BeckOK InfoMedienR, § 1, TMG Rn. 8.
[88] Martini in BeckOK InfoMedienR, § 1 TMG, Rn. 8.
[89] Ricke in Spindler/Schuster, § 1 TMG, Rn. 4.
[90] BT-Drucks. 16/3078, S. 13.
[91] BT-Drucks. 16/3078, S. 13 f.

Begriffsbestimmung der Telekommunikationsdienste, telekommunikationsgestützten Dienste und des Rundfunks erforderlich.

a) Telekommunikationsdienste

Telekommunikationsdienste im Sinne des § 3 Nr. 24 TKG sind Dienste, die in der Regel gegen Entgelt erbracht werden und die ganz oder überwiegend in der Übertragung von Signalen über Telekommunikationsnetze bestehen, einschließlich Übertragungsdienste in Rundfunknetzen. Unter Telekommunikationsnetzen ist die Gesamtheit von Übertragungssystemen und gegebenenfalls Vermittlungs- und Leitwegeinrichtungen sowie anderweitigen Ressourcen zu verstehen, einschließlich der nicht aktiven Netzbestandteile, die die Übertragung von Signalen über Kabel, Funk, optische und andere elektromagnetische Einrichtungen ermöglichen, einschließlich Satellitennetzen, festen, leitungs- und paketvermittelten Netzen, einschließlich des Internets, und mobilen terrestrischen Netzen, Stromleitungssystemen, soweit sie zur Signalübertragung genutzt werden, Netzen für Hör- und Fernsehfunk sowie Kabelfernsehnetzen, unabhängig von der Art der übertragenen Information (§ 3 Nr. 27 TKG).

Damit fallen unter den Begriff jegliche Anbieter von Telefonie, auch Internet-Telefonie[92], sowie Internet-Zugangsanbieter, sog. Access-Provider, und Anbieter von E-Mail-Übertragungsdiensten. Voraussetzung ist allerdings, dass der Anbieter seinen Schwerpunkt in der technischen Transportleistung hat und nicht in der Vermittlung von Inhalten. Denn der Begriff der Telekommunikation erfasst lediglich den technischen Vorgang des Aussendens, Übermittelns und Empfangens von Signalen (§ 3 Nr. 22 TKG).

Da sich insbesondere im Bereich der Zugangsvermittlung zum Internet und der E-Mail-Übertragung die Tätigkeit der Anbieter nicht nur auf die technische Übertragung von Signalen beschränkt,

[92] Sog. Voice over Internet Protocol-Dienste (VoIP).

sondern von diesen oftmals noch weitere inhaltliche Leistungen angeboten werden, können diese sowohl unter den Anwendungsbereich des TKG als auch des TMG fallen.[93] § 1 Abs. 1 S. 1 TMG nimmt lediglich solche Dienste des § 3 Nr. 24 TKG aus dem Anwendungsbereich heraus, welche ganz in der Übertragung von Signalen über Telekommunikationsnetze bestehen und nicht solche, die lediglich überwiegend darin bestehen.[94]

b) Telekommunikationsgestützte Dienste

Telekommunikationsgestützte Dienste sind nach der Legaldefinition des § 3 Nr. 25 TKG solche, die keinen räumlich und zeitlich trennbaren Leistungsfluss auslösen, sondern bei denen die Inhaltsleistung noch während der Telekommunikationsverbindung erfüllt wird. Dies sind folglich Dienste, bei denen im Rahmen einer Telekommunikationsverbindung zusätzliche Leistungen erbracht werden (sog. Mehrwertdienste).[95] Ein klassisches Beispiel sind sog. 0900er Rufnummern, der Nachfolger der bekannten 0190er Rufnummern[96]. Hier werden Dienstleistungen über die Telekommunikationsverbindung erbracht und die Vergütung dafür wird über die Telefonrechnung eingezogen.[97]

c) Rundfunk

Nach der Legaldefinition des § 2 Abs. 1 RStV ist Rundfunk ein linearer Informations- und Kommunikationsdienst. Er ist die für die Allgemeinheit und zum zeitgleichen Empfang bestimmte Veranstaltung und Verbreitung von Angeboten in Bewegtbild oder Ton entlang eines Sendeplans unter Benutzung elektromagnetischer Schwingungen. Der Begriff schließt Angebote ein, die verschlüsselt verbreitet werden oder gegen besonderes Entgelt empfangbar sind.

---

[93] So auch in BT-Drucks. 16/3078, S. 13.
[94] Martini in BeckOK InfoMedienR, § 1 TKG, Rn. 11.
[95] Ditscheid/Rudloff in BeckTKG-Kommentar, § 1 Rn. 81.
[96] 0190er Rufnummern hatten früher u.a. einen Ruf als teure Erotik-Hotlines.
[97] Härting, DB 2002, 2147, 2147.

Das zentrale Merkmal, welches den Rundfunk von den Telekommunikationsdiensten und Telemedien abgrenzt, ist das der Linearität.[98]

§ 2 Abs. 3 RStV enthält zudem einen Negativkatalog von Angeboten, die nicht dem Rundfunk zugeordnet werden. Es handelt sich hierbei um Angebote (a) für weniger als 500 potenzielle Rezipienten, (b) die zur unmittelbaren Wiedergabe aus Speichern von Empfangsgeräten bestimmt sind, (c) die ausschließlich persönlichen oder familiären Zwecken dienen, (d) die nicht journalistisch-redaktionell gestaltet sind oder (e) die aus Sendungen bestehen, die jeweils gegen Einzelentgelt freigeschaltet werden.

III. Internet Service Provider

Das TMG selbst verwendet nicht den Begriff des Internet Service Providers, sondern den des „Diensteanbieters". Inhaltlich sind diese beiden Begriffe aber identisch. Ebenso ist es im allgemeinen Sprachgebrauch üblich, allgemein vom Provider zu sprechen.

Diensteanbieter ist nach der Legaldefinition jede natürliche oder juristische Person, die eigene oder fremde Telemedien zur Nutzung bereithält oder den Zugang zur Nutzung vermittelt bzw. bei audiovisuellen Medieninhalten auf Abruf, jede natürliche oder juristische Person, die die Auswahl und Gestaltung der angebotenen Inhalte wirksam kontrolliert.[99]

Da der Begriff der Diensteanbieter bzw. der ISP demnach ein weites Spektrum von Diensten erfasst, ist es insbesondere für die Frage der haftungsrechtlichen Verantwortung notwendig, eine weitere Unterscheidung vorzunehmen. Das TMG differenziert in seinen Normen grundsätzlich zwischen dem Content-Provider[100], dem Access-Provider[101], dem Cache-Provider[102] und dem Host-Provider[103].

---

[98] Martini in BeckOK InfoMedienR, § 2 RStV, Rn. 3.
[99] § 2 S. 1 Nr. 1 TMG.
[100] § 7 Abs. 1 TMG.
[101] § 8 TMG.
[102] § 9 TMG.
[103] § 10 TMG.

1. Content-Provider

Der Content-Provider[104] stellt eigene Inhalte zur Nutzung zur Verfügung und ist nach den allgemeinen Gesetzen für diese Inhalte vollumfänglich verantwortlich. Für ihn greifen nicht die Haftungsprivilegien des TMG.

2. Host-Provider

Der Hostprovider[105] stellt seinen Nutzern auf seinen Servern Speicherplatz für deren eigene Inhalte zur Verfügung. Hiervon umfasst werden Betreiber von Plattformen für das Einstellen von Audio-, Video- oder Bilddateien, wie bspw. YouTube, Pinterest oder Tumblr. Der Begriff erfasst aber auch soziale Netzwerke, wie bspw. Facebook und Twitter sowie Auktionsplattformen wie eBay.
Auch File-Hosting-Dienste bzw. Share-Hosting-Dienste[106] fallen unter diese Kategorie. Diese stellen ihren Nutzern Speicherplatz auf ihren Servern zur Verfügung, im Unterschied zu den oben genannten Plattformen wird dem Nutzer, nach dem dieser die jeweilige Datei hochgeladen hat, aber lediglich ein Link übermittelt, mit dem die hochgeladene Datei aufgerufen und heruntergeladen werden kann.[107]
Immer beliebter werden Online-Speicher, bei denen dem Nutzer ein konkret festgelegtes Datenvolumen mittels sog. Cloud-Computing Technologie zur Verfügung gestellt wird.[108] Hierbei werden Daten oder Programme in externen Rechenzentren gespeichert bzw. ausgeführt und dem Nutzer lediglich auf seinem Computer angezeigt, es erfolgt keine lokale Speicherung auf dem Computer des Nutzers.[109] Der Cloud-Provider speichert die Inhalte für den Nutzer in einer sog. „Cloud“ und teilt dem Nutzer lediglich

[104] Vom englischen Begriff „content“ = Inhalt.
[105] Auch Webhost-Provider oder Hosting-Provider genannt, vom englischen Begriff „to host“ = bewirten, Gastgeber sein.
[106] Kurz auch Filehoster/Sharehoster genannt.
[107] BGH MMR 2013, 733, 733.
[108] Ballhausen/Roggen in Kilian/Heussen, Providerverträge, Rn. 21.
[109] Bisges, MMR 2012, 574, 574.

die ihm zugewiesene Adresse mit, unter welcher der Speicherplatz dauerhaft erreichbar ist und die Inhalte abrufbar sind.[110]

3. Cache-Provider

Der Cache-Provider[111] speichert Inhalte des Nutzers automatisch und lediglich zeitlich begrenzt zwischen, um die Übermittlung dieser Inhalte an andere Nutzer effizienter zu gestalten.

Die Inhalte werden auf sog. Proxy-Cache-Servern gespeichert, so dass sie bei erneutem Aufruf der Seite durch den Nutzer direkt von diesem Server abgerufen werden und nicht mehr vom Quell-Server, von dem diese Inhalte ursprünglich stammen.[112]

Vorteile dieser Zwischenspeicherung sind die schnellere Zugriffsmöglichkeit auf den Inhalt sowie die damit zusammenhängende geringere Netzbelastung und die dadurch reduzierten Verbindungskosten.[113]

4. Access-Provider/Network-Provider

Der Access-Provider[114] vermittelt den Nutzern den Zugang zum Internet.

Gem. § 1 Abs. 1 S. 1 TMG sind Telekommunikationsdienste nach § 3 Nr. 24 TKG, die ganz in der Übertragung von Signalen über Telekommunikationsnetze bestehen, vom Geltungsbereich des TMG ausgenommen sind. Der Access-Providern hingegen ist ein Telekommunikationsdienst, der nicht ganz sondern nur überwiegend in der Übertragung von Signalen über Telekommunikationsdienstleistungen besteht, da er neben der Übertragungsdienstleistung auch eine inhaltliche Dienstleistung anbietet, nämlich den Internetzugang anbietet. [115] Er kann daher sowohl als Telekommunikationsdienst im Sinne des TKG als auch als Telemedium im Sinne des TMG klassifiziert werden.[116]

---

[110] Ballhausen/Roggen in Kilian/Heussen, Providerverträge, Rn. 21 f.
[111] Auch Proxy-Cache-Provider genannt, vom englischen Begriff „to cache“ = puffern, zwischenspeichern.
[112] Hoffmann in Spindler/Schuster, § 9 TMG Rn. 1 f.
[113] Sieber in Hoeren/Sieber/Holznagel, Teil 1, Rn. 27.
[114] Vom englischen „access“ = Zugang.
[115] BT-Drucks. 16/3078, S. 13.
[116] Schütz in BeckTKG-Kommentar, § 6 Rn. 25.

Der Begriff der Access-Provider erfasst daher sowohl große Telekommunikationsunternehmen wie T-Online als auch Kabelnetzbetreiber wie Kabel Deutschland sowie Mobilfunkunternehmen wie E-Plus, die einen Internetzugang über ihre Mobilfunknetze anbieten.

Der Network-Provider[117] übermittelt Informationen seiner Nutzer in einem Kommunikationsnetz. Er hält die Telekommunikationsinfrastruktur bereit und bietet dem Nutzer die Nutzung seiner Übertragungskapazitäten an.[118] Hierunter fällt bspw. das Weiterleiten der Kopie einer abgerufen Webeseite oder von E-Mails eines Anbieters von E-Mail-Diensten.[119] Auch er erbringt neben der Übertragungsdienstleistung eine inhaltliche Dienstleistung.[120]

C. Verantwortlichkeit und Privilegien der ISP in Deutschland

Dieser Teil behandelt etwaig bestehende Privilegien der ISP, deren Verantwortlichkeit nach den allgemeinen Gesetzen sowie potentielle Mitwirkungspflichten der ISP in Deutschland.

I. Haftungsprivilegien nach §§ 7 ff. TMG

Die Haftungsprivilegien der ISP sind derzeit unter Abschnitt 3 „Verantwortlichkeit“ in §§ 7-10 TMG zu finden. Anders als der Wortlaut „Verantwortlichkeit“ des 3. Abschnitts dies impliziert, begründen die §§ 7-10 TMG allerdings keine Verantwortlichkeiten der ISP im Sinne einer Garantenstellung[121], sondern legen vielmehr die Voraussetzungen fest, unter welchen diese eine Haftungsprivilegierung für sich beanspruchen können und haben damit haftungsbeschränkenden Charakter im Hinblick auf die zivil- und strafrechtliche Verantwortlichkeit.[122]

---

[117] Deutsch: Netzwerkbetreiber.
[118] Altenhain in MüKo zum StGB, § 1 TMG, Rn. 15.
[119] Altenhain in MüKo zum StGB, Vorbemerkung zu den §§ 7 ff. TMG, Rn. 52.
[120] BT-Drucks. 16/3078, S. 13.
[121] Altenhain in MüKo zum StGB, § 7 TMG, Rn. 6; S. hierzu näher S. 124.
[122] BT-Drucks. 14/6098, S. 23 und S. 37.

1. Gesetzgebungsgeschichte

Durch Einführung von Privilegien der ISP im Jahr 1997 nahm Deutschland eine Vorreiterrolle ein.

Im Zuge der Entwicklung und Verbreitung neuer Informations- und Kommunikationsdienste sah der Gesetzgeber sich dazu veranlasst, Regelungen zu schaffen, die einheitliche Rahmenbedingungen für die neuen Geschäftsmodelle festlegen. Hierdurch sollten Investitionshemmnisse für die Anbieter solcher Geschäftsmodelle abgebaut werden, um damit auf längere Sicht den Wirtschaftsstandort Deutschland zu fördern und zukunftsfähig zu gestalten.[123]

a) IuKDG

Da sowohl der Bund als auch die Länder jeweils die Gesetzeskompetenz für das Internet für sich beanspruchten, einigte man sich zunächst durch das IuKDG[124] auf zwei unterschiedliche Regelungen zur Haftungsprivilegierung der ISP. Der Bund stellte seine Kompetenz für sog. Teledienste im Teledienstegesetz (TDG a.F.) klar, während die sog. Mediendienste in die Zuständigkeit der Länder fielen und entsprechend im Staatsvertrag über Mediendienste (MDStV a.F.) geregelt wurden.[125] Teledienste waren demnach Dienste für eine individuelle Nutzung auf der Grundlage einer Übermittlung mittels Telekommunikation, wie bspw. Telebanking oder Telespiele, während Mediendienste sich an die Allgemeinheit richteten unter Benutzung elektromagnetischer Schwingungen, wie bspw. Teleshopping.

Die Haftungsprivilegien für ISP fanden schließlich Einzug in § 5 Abs. 1 TDG a.F. bzw. § 5 MDStV a.F.

---

[123] BT-Drucks. 13/7385, S. 18.

[124] Gesetz zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste (Informations- und Kommunikationsdienste-Gesetz – IuKDG) vom 22. 7. 1997 (BGBl. I S. 1870).

[125] Siehe hierzu auch die gemeinsame Erklärung von Bund und Ländern vom 18.12.1996, abgedruckt in Engel-Flechsig, ZUM 1997, 231 ff.

b) EGG

Mit dem EGG[126] wurde 2001 die europäische ECRL[127] umgesetzt. Der europäische Richtliniengeber hat die Bedeutung eines einheitlichen Rechtsrahmens für Dienste des elektronischen Geschäftsverkehrs innerhalb des Binnenmarktes erkannt und in der Folge Vorschriften bezüglich Haftungsprivilegien für ISP seinen Mitgliedsstaaten zur Umsetzung auferlegt. Ziele waren der Anreiz für Investitionen in Innovationen sowie die Stärkung der Wettbewerbsfähigkeit der europäischen Wirtschaft.[128]

Die Vorschriften der ECRL hinsichtlich der ISP-Privilegien wurden in §§ 8-11 TDG n.F. sowie §§ 6-9 MDStV n.F. umgesetzt und waren gegenüber ihren Vorgängervorschriften um einiges umfassender und detaillierter.

c) EIGVG

Nachdem sich Bund und Länder 2004 auf eine Zusammenführung der wirtschaftsbezogenen Regelungen für Tele- und Mediendienste geeinigt hatten, wurde durch das EIGVG[129] das TDG aufgehoben und durch das TMG ersetzt. Die Länder hoben entsprechend den MDStV auf und regelten die inhaltlichen Anforderungen nunmehr im RStV.

Inhaltliche Änderungen der Privilegierungsvorschriften des TMG gegenüber dem TDG und MDStV ergaben sich hierdurch allerdings nicht.

---

[126] Gesetz über rechtliche Rahmenbedingungen für den elektronischen Geschäftsverkehr – Elektronischer Geschäftsverkehr-Gesetz.

[127] Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates vom 8. Juni 2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmark – E-Commerce-Richtlinie.

[128] Erwägungsgrund (2) der ECRL.

[129] Gesetz zur Vereinheitlichung von Vorschriften über bestimmte elektronische Informations- und Kommunikationsdienste - Elektronischer-Geschäftsverkehr-Vereinheitlichungsgesetz.

2. Anwendungsbereich

Die §§ 7-10 TMG gelten horizontal, d.h. für alle Rechtsgebiete, und umfassen somit sowohl zivilrechtliche als auch strafrechtliche Ansprüche.[130]

Umstritten ist allerdings die Anwendbarkeit der Privilegien auf negatorische Ansprüche.[131]

3. Adressaten

Die Adressaten der §§ 7-10 TMG sind die dort aufgeführten Diensteanbieter. Handelt es sich bei dem Diensteanbieter um ein Unternehmen, so ist jedoch nicht lediglich der Inhaber des Unternehmens von der Haftung privilegiert, sondern auch seine Mitarbeiter.[132] Würde man Mitarbeiter nicht den Privilegien unterwerfen, würde dies zu dem widersprüchlichen Ergebnis führen, dass dem Unternehmen das Haftungsprivileg faktisch wieder entzogen werden würde.[133] Eine solche Auslegung würde somit dem Zielen der ECRL entgegenstehen.[134] Aus diesem Grund sind die Mitarbeiter eines Unternehmens, welches Dienste nach §§ 7-10 TMG zur Verfügung stellt, gleichsam als Adressaten der

[130] BT-Drucks. 14/6098, S. 23. Klarstellend auch noch mal Erwägungsgrund 16 der InfoSoc-RL: „*Die Haftung für Handlungen im Netzwerk-Umfeld betrifft nicht nur das Urheberrecht und die verwandten Schutzrechte, sondern auch andere Bereiche wie Verleumdung, irreführende Werbung, oder Verletzung von Warenzeichen, und wird horizontal in der Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates vom 8. Juni 2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt („Richtlinie über den elektronischen Geschäftsverkehr“) geregelt, die verschiedene rechtliche Aspekte der Dienste der Informationsgesellschaft, einschließlich des elektronischen Geschäftsverkehrs, präzisiert und harmonisiert. Die vorliegende Richtlinie sollte in einem ähnlichen Zeitrahmen wie die Richtlinie über den elektronischen Geschäftsverkehr umgesetzt werden, da jene Richtlinie einen einheitlichen Rahmen für die Grundsätze und Vorschriften vorgibt, die auch für wichtige Teilbereiche der vorliegenden Richtlinie gelten. Die vorliegende Richtlinie berührt nicht die Bestimmungen der genannten Richtlinie zu Fragen der Haftung.*“

[131] Siehe hierzu eingehend S. 62.

[132] Altenhain in MüKo zum StGB, Vorbemerkung zu den §§ 7 ff., Rn. 13; Sieber/Höfinger in Hoeren/Sieber/Holznagel, Teil 18.1 Rn. 35.

[133] Altenhain in MüKo zum StGB, Vorbemerkung zu den §§ 7 ff., Rn. 13; Sieber/Höfinger in Hoeren/Sieber/Holznagel, Teil 18.1 Rn. 35.

[134] Altenhain in MüKo zum StGB, Vorbemerkung zu den §§ 7 ff., Rn. 13; Sieber/Höfinger in Hoeren/Sieber/Holznagel, Teil 18.1 Rn. 35.

Bestimmungen anzusehen, sofern sie in Ausübung der ihnen übertragenen Aufgaben tätig werden.[135]

4. Dogmatische Einordnung

Die dogmatische Einordnung der Haftungsprivilegien ist bereits seit ihrer Einführung durch das IuKDG Gegenstand reger Diskussion vor allem im Schrifttum. Dabei stehen sich sog. einstufige und zweistufige Modelle gegenüber. Während die Privilegien bei dem einstufigen Modell in das Prüfungssystem der jeweiligen Anspruchsnorm integriert sind und innerhalb dieser geprüft werden, sieht das zweistufige Modell eine gesonderte Prüfung von Privilegien und jeweils einschlägiger Haftungsnorm vor.

a) Einstufiges Modell

Bei dem einstufigen Modell werden die Voraussetzungen einer Privilegierung nach TMG entweder auf Tatbestands-, Rechtswidrigkeits- oder Schuldebene verortet.

aa) Schuldebene

In einem frühen Urteil des LG München I aus dem Jahre 1999 hat das Gericht, entgegen der damals schon herrschenden Auffassung einer Filterfunktion, die Privilegien in den klassischen Aufbau einer strafrechtlichen Norm (Tatbestand – Rechtswidrigkeit – Schuld) eingebaut und hier im Rahmen der Schuldfrage geprüft.[136] Als Begründung wurde vornehmlich auf die im TMG (damals noch TDG a.F.) enthaltenen Begriffe der „Kenntnis“ und „Verantwortlichkeit“ abgestellt, welche darauf hindeuten würden, dass die Privilegien nur auf der Schuldebene angesiedelt werden könnten.

Diese Ansicht hat sich jedoch nicht durchgesetzt. Dies ist insbesondere im Hinblick auf die vor allem im Bereich des Urheberrechts verschuldensunabhängigen Ansprüche auf Unterlassung und Beseitigung bedeutsam.

---

[135] Altenhain in MüKo zum StGB, Vorbemerkung zu den §§ 7 ff., Rn. 13.
[136] LG München I, CR 2000, 117, 119.

Zudem würde diese Zuordnung der Intention des Gesetzgebers zuwiderlaufen, der mit der Schaffung der Privilegien gerade die Sozialadäquanz der Tätigkeit des ISP statuieren wollte. Eine Einordnung auf Schuldebene würde hingegen nicht die Tätigkeit vom Tatbestand der einschlägigen Norm ausschließen, sondern lediglich im Einzelfall eine Verantwortlichkeit des ISP mangels Schuld entfallen lassen.[137]

bb) Rechtswidrigkeitsebene

Auch die Ansiedlung der Privilegien innerhalb der Prüfung der Rechtswidrigkeit scheidet vor dem Hintergrund der gesetzgeberischen Intention aus.[138] Denn dies würde bedeuten, dass ein an sich sozialwidriges Verhalten des ISP lediglich im Einzelfall aufgrund besonderer Umstände gerechtfertigt ist.[139]

cc) Tatbestandsebene

Die Befürworter eines einstufigen Modells gehen vornehmlich von einer Prüfung innerhalb des jeweils einschlägigen Tatbestandes aus.[140] Dies hätte zur Folge, dass die jeweiligen rechtsgebietsspezifischen allgemeinen Regeln auch auf die Haftungsprivilegien anwendbar sind.[141]

Unterschiedliche Auffassungen gibt es lediglich darüber, wo genau innerhalb des Tatbestandes die Privilegierungsvoraussetzungen zu verorten sind. Denkbar ist sowohl eine „tatbestandsintegrierte Vorfilterlösung“ als auch eine sog. „Integrationslösung“. Erstere kennzeichnet die vorgelagerte Prüfung der Privilegien innerhalb

---

[137] So auch Hoffmann in Spindler/Schuster, Vorbemerkung § 7 - § 10 TMG, Rn. 31; Sieber/Höfinger in Hoeren/Sieber/Holznagel, Teil 18.1, Rn. 24.

[138] A.A. wohl Freytag, ZUM 1999, 185, 189, jedenfalls zur Regelung des § 5 TDG a.F./§ 5 MDStV a.F., der eine Einordnung auf Rechtswidrigkeitsebene zumindest für denkbar hält, einer Einordnung auf Tatbestandsebene im Rahmen der Zurechnung dann aber den Vorrang einräumt.

[139] So auch Hoffmann in Spindler/Schuster, Vorbemerkung § 7 - § 10 TMG, Rn. 32; Sieber/Höfinger in Hoeren/Sieber/Holznagel, Teil 18.1, Rn. 23.

[140] Hoffmann in Spindler/Schuster, Vorbemerkung § 7 - § 10 TMG, Rn. 32; Sieber/Höfinger in Hoeren/Sieber/Holznagel, Teil 18.1, Rn. 25; Bettinger/Freytag, CR 1998, 545, 548; Freytag, ZUM 1999, 185, 189; Spindler, CR 2004, 50, 51.

[141] Sieber, Rn. 250, im Bereich des Strafrechts bspw. das Bestimmtheitsgebot, das Analogieverbot und Irrtumsregeln, im Bereich des Zivilrechts bspw. die Wissenszurechnung Dritter.

des jeweils einschlägigen Tatbestandes.[142] Letztere verortet die Merkmale der Privilegien in die jeweiligen Merkmale der Haftungsnorm und modifiziert diese dadurch.[143] Der überwiegende Teil der Literatur sieht die Privilegien innerhalb des objektiven Zurechnungszusammenhangs im Sinne einer „tatbestandsintegrierten Vorfilterlösung".[144] Die genaue Einordnung hat jedoch keine praktische Bedeutung, sowohl die „Vorfilterlösung" als auch die „Integrationslösung" werden zu dem gleichen Ergebnis gelangen.[145]

b) Zweistufiges Modell

Das zweistufige Modell sieht eine getrennte Prüfung von Privilegien des TMG und der jeweils haftungsbegründenden Norm vor.

aa) Nachfilter

Die Begründung des Gesetzesentwurfs des EGG vergleicht die Wirkungsweise der Privilegien mit der eines Filters. Aus dem genauen Wortlaut der Begründung wurde vereinzelt die Einordnung als sog. Nachfilter herausgelesen.[146] Gestützt wurde diese Ansicht auf den folgenden Satz: *„Sind daher im Einzelfall die Voraussetzungen der allgemeinen Vorschriften für eine Haftung erfüllt, so ist der Diensteanbieter für die Rechtsgutsverletzung gleichwohl nicht verantwortlich, wenn er sich auf das Eingreifen der §§ 9,10 oder 11 berufen kann."*[147]

Diese Leseart der Gesetzesbegründung vernachlässigt aber die dem Satz vorangestellte Erläuterung *„Bevor ein Diensteanbieter auf deren [den allgemeinen Vorschriften, Anmerkung des Verfassers] Grundlage zur Verantwortung gezogen werden kann, muss*

[142] So z.B. Sieber/Höfinger in Hoeren/Sieber/Holznagel, Teil 18.1, Rn. 26; Blanke, S. 190; Sieber, Rn. 246.
[143] So z.B. Freytag, ZUM 1999, 185, 189; Sobola/Kohl, CR 2005, 443, 445.
[144] Hoffmann in Spindler/Schuster, Vorbemerkung § 7 - § 10 TMG, Rn. 32; Sieber/Höfinger in Hoeren/Sieber/Holznagel, Teil 18.1, Rn. 26; Sieber, Rn. 246 f.
[145] Sieber, Rn. 246.
[146] Bornkamm/Seichter, CR 2005, 747, 749; Hoffmann, MMR 2002, 284, 285; Sobola/Kohl, CR 2005, 443, 445.
[147] BT-Drucksache 14/6098, S. 23.

allerdings geprüft werden, ob die aus den allgemeinen Vorschriften folgende Verantwortlichkeit nicht durch die §§ 9 bis 11 ausgeschlossen ist", welche eindeutig dafür spricht in einem ersten Schritt die Privilegien zu prüfen und erst in einem zweiten Schritt, sollten diese verneint werden, die allgemeinen Haftungsvorschriften heranzuziehen.

bb) Vorfilter

Die h.M. in Literatur sieht die Privilegien deshalb als sog. Vorfilter.[148] Erst wenn die Voraussetzungen für eine Privilegierung nicht gegeben sind, kann der ISP gemäß den allgemeinen Gesetzen zur Verantwortung gezogen werden.

Auch der BGH hat sich dieser Sichtweise im Hinblick auf § 5 TDG a.F. unter Bezugnahme auf die Gesetzesbegründung zum IuKDG angeschlossen.[149] Die Privilegierungsregelungen seien der straf- und zivilrechtlichen Prüfung vorgelagert.[150] Deshalb dürfe diese erst in einem zweiten Schritt erfolgen, nachdem die grundsätzliche Verantwortlichkeit der ISP festgestellt wurde.[151]

Die Einordnung als ein von der jeweils einschlägigen Haftungsnorm unabhängiger Filter überzeugt auch für die durch das EGG modifizierten Haftungsprivilegien in europarechtlicher Hinsicht.

Die Privilegien sollten bestehende und sich entwickelnde Unterschiede der Providerhaftung in den Mitgliedsstaaten im Rahmen einer Vollharmonisierung beseitigen, das heißt die Mitgliedsstaaten dürfen weder weitere noch engere Regelungen innerhalb der nationalen Gesetze vorsehen.[152] Die auf Grundlage der ECRL erlassenen Regelungen sind sodann europäisch-autonom

---

[148] Altenhain in MüKo zum StGB, Vorbemerkung zu den §§7 ff., Rn. 7; Müller-Broich, Vor §§7-10, Rn. 1; Wabnitz/Janovsky/Dannecker/Bülte/Möhrenschlager in Wabnitz/Jankovsky, C. Straftaten im Internet, Rn. 192; Hollenders, S. 205; Engel-Flechsig/Maennel/Tettenborn, NJW 1997, 2981, 2984; Gercke, CR 2006, 844, 848; Tettenborn/Bender/Lübben/Karenfort/Santelmann/Enaux/König, K u. R 2001, Beilage, 1, 27.

[149] BGH MMR 2004, 166, 167.

[150] BGH MMR 2004, 166, 167.

[151] BGH MMR 2004, 166, 167.

[152] Marly in Grabitz/Hilf, Band IV, ECRL Vorbemerkungen zu Abschnitt 4, Rn. 3.

auszulegen, das heißt, dass nationale Auslegungsgrundsätze dahinter zurücktreten.[153]

Aus diesem Grund geht auch der Einwand der Vertreter einer tatbestandsintegrierten Verortung der Privilegien, dass bei einer Prüfung außerhalb des jeweils einschlägigen Tatbestandes nicht die für die Tatbestandsmerkmale geltenden allgemeinen Regeln auf die Haftungsregelung Anwendung finden, fehl. Insbesondere der Einwand, dass nur durch die Einordnung innerhalb der jeweiligen Haftungsnorm sichergestellt werden könne, dass die strafrechtlichen Irrtums- und Teilnahmeregeln bei der Prüfung der Haftungsprivilegien des TMG greifen[154], überzeugt nicht.

Vielmehr steht einer derartigen Auslegung bereits der der Begründung der Haftungsprivilegien zugrundeliegende Gedanke einer einheitlichen Verantwortlichkeitsregelung im Sinne einer Querschnittsregelung, welche gleichermaßen für alle Rechtsgebiete Geltung beansprucht, entgegen. Nach der Intention des europäischen Richtliniengebers sollten bestehende und sich entwickelnde Unterschiede bezüglich der Verantwortlichkeit der ISP innerhalb der Mitgliedsstaaten beseitigt werden.[155] Dieses Ziel lässt sich allerdings nur mit einer von nationalen teilrechtsgebietsimmanenten Grundsätzen unabhängigen Prüfung erreichen, da nur diese die gewünschte Rechtseinheit schafft sowie dem Querschnittscharakter der Regelungen gerecht wird.

Soweit kritische Stimmen in der Literatur eine dadurch auftretende Doppelprüfung monieren, weist *Altenhain* zu Recht daraufhin, dass etwaige, bei einer Doppelprüfung einzelner Voraussetzungen auftretende Unterschiede eben nicht widersprüchlich sind, sondern in der Natur der Sache einer zweistufig aufgebauten Prüfung liegen.[156] So ist es durchaus möglich, dass auf der ersten Stufe bei der allgemeinen Prüfung der Verantwortlichkeit die Kenntnis des

---

[153] Marly in Grabitz/Hilf, Band IV, ECRL Vorbemerkung: Der elektronische Geschäftsverkehr als Gegenstand der Richtlinie 2000/31/EG, Rn. 60.

[154] So z.B. Blanke, S. 190; Hilgendorf, NStZ 2000, 518, 519; Satzger, CR 2001, 109, 110 f.

[155] S. hierzu auch Erwägungsgrund (40) der ECRL.

[156] Altenhain in MüKo zum StGB, Vorbemerkung zu den §§ 7 ff., Rn. 8.

Host-Providers im Rahmen des § 10 TMG bejaht wird, während auf der zweiten Stufe im Rahmen einer strafrechtlichen Prüfung des § 106 UrhG eine Kenntnis aufgrund nicht möglicher Wissenszurechnung verneint wird. Dass der ISP nicht nach dem TMG privilegiert ist, bedeutet nicht zugleich, dass er nach den allgemeinen Gesetzen verantwortlich ist.
Zudem kommt es lediglich zu einer etwaigen Doppelprüfung, wenn die Voraussetzungen für eine Haftungsprivilegierung zunächst nicht vorliegen.

5. Einzelne Privilegierungstatbestände

Wie bereits eingangs dargestellt, liegt den Privilegierungsvorschriften des TMG ein abgestuftes Haftungssystem zugrunde, basierend auf den unterschiedlichen Tätigkeitsbereichen der ISP und ihrer damit einhergehenden Nähe zur beanstandeten Information. Entsprechend knüpft die Privilegierung der verschiedenen ISP an unterschiedliche Voraussetzungen an. Insgesamt bestimmt das TMG drei unterschiedliche Aufgabenbereiche, die (1) Durchleitung von Informationen, § 8 TMG, (2) Zwischenspeicherung zur beschleunigten Übermittlung von Informationen, § 9 TMG und (3) Speicherung von Informationen, § 10 TMG.

a) Allgemeine Grundsätze

Gleichermaßen verbindlich für alle ISP sind die in § 7 Abs. 2 TMG geregelten allgemeinen Grundsätze.

aa) Keine allgemeine Überwachungs- und Nachforschungspflicht

§ 7 Abs. 2 S. 1 TMG bestimmt, dass Diensteanbieter im Sinne der §§ 8 bis 10 TMG nicht verpflichtet sind, die von ihnen übermittelten oder gespeicherten Informationen zu überwachen oder nach Umständen zu forschen, die auf eine rechtswidrige Tätigkeit hinweisen. Der deutsche Gesetzgeber hat damit nahezu wörtlich Artikel 15 Abs. 1 ECRL umgesetzt, der derartige „allgemeine Verpflichtungen“ untersagt.

Der ISP muss demnach keine anlassunabhängige, pro-aktive Überprüfung seiner Dienste vornehmen, um etwaige dort vorhandene Rechtsverletzungen aufzudecken.[157]

(1) EuGH-Urteile: SABAM/Scarlet[158] und SABAM/Netlog[159]

Der EuGH befasste sich innerhalb kurzer Zeit gleich zweimal mit dem Verbot einer allgemeinen Überwachungspflicht nach Art. 15 Abs. 1 ECRL und dessen Vereinbarkeit mit gerichtlich auferlegten Anordnungen zur Unterlassung. In SABAM/Scarlet ging die belgische Verwertungsgesellschaft SABAM gegen den Anbieter eines Internetzugangsdienstes vor und verlangte, dass dieser es seinen Kunden unmöglich mache, Dateien, welche Werke aus dem SABAM-Repertoire beinhalten, in irgendeiner Form mit Hilfe eines Peer-to-Peer-Programms zu senden oder zu empfangen oder eine solche Möglichkeit zu blockieren.

SABAM/Netlog betraf den Betreiber eines sozialen Netwerks, den SABAM dazu verpflichten wollte, es künftig zu unterlassen, der Öffentlichkeit ohne Genehmigung Werke aus dem SABAM-Repertoire zur Verfügung zu stellen.

Der EuGH urteilte in beiden Verfahren, dass eine solche Anordnung gegen Art. 15 Abs. 1 ECRL verstoße.

Im Falle von Scarlet führte das Gericht aus, dass eine solche Anordnung auf Filterung des Datenverkehrs eine aktive Überwachung sämtlicher elektronischer Kommunikation im Netz des Providers erfordern würde und dadurch jede zu übermittelnde Information eines jeden das Netz nutzenden Kunden erfasst wäre.[160] Die Anwendung des Filtersystems würde bedeuten, dass der Access-Provider sämtliche durchgeleiteten Informationen identifiziere, unter diesen Dateien ermittele, welche Dateien unzulässig sind und die von ihm als unzulässig qualifizierten

[157] Altenhain in MüKo zum StGB, § 7 Rn. 6.
[158] EuGH GRUR 2012, 265 - Urteil vom 24.11.2011 – C-70/10 „Scarlet SABAM“ = Slg. I 2011, 12006.
[159] EuGH GRUR 2012, 382 – Urteil vom 16.02.2012 – C-360/10 „SABAM/Netlog“.
[160] EuGH GRUR 2012, 265, 267 (Rn. 39).

Dateien sperre.[161] Diese Verpflichtung einer präventiven Überwachung würde eine aktive Beobachtung sämtlicher Daten aller Kunden erfordern und sei nach Art. 15 Abs. 1 ECRL unzulässig.[162] Die Anordnung würde zudem die widerstreitenden Grundrechte nicht ausreichend berücksichtigen.[163] Die Anordnung zur Errichtung eines komplizierten, kostspieligen, auf Dauer angelegten und auf Kosten des Access-Providers betriebenen Systems würde eine qualifizierte Beeinträchtigung der unternehmerischen Freiheit des Access-Providers bedeuten.[164] Des Weiteren würde die Anordnung das Datenschutzrecht der Nutzer beeinträchtigen, da das streitgegenständliche Filtersystem die Sammlung und Identifizierung der IP-Adressen der Nutzer erfordere, sowie das Recht auf freien Empfang bzw. die freie Sendung von Informationen, da das System möglicherweise nicht hinreichend zwischen rechtmäßigen und unrechtmäßigen Inhalten unterscheiden könne.[165]

Auch in SABAM/Netlog lehnte der Gerichtshof eine solche Anordnung aus den gleichen Gründen ab. Die Anordnung würde eine aktive Beobachtung der von allen Nutzern auf der Plattform gespeicherten Daten erfordern.[166] Die Einrichtung des hierfür erforderlichen Filtersystems, um jeder künftigen Urheberrechtsverletzung vorzubeugen sei nicht mit Art. 15 Abs. 1 ECRL vereinbar.[167] Zudem würde die Anordnung zur Einrichtung des Filtersystems das Erfordernis der Gewährleistung eines angemessenen Gleichgewichts zwischen den widerstreitenden Grundrechten missachten.[168]

(2) Bewertung der EuGH-Urteile

Den Urteilen des EuGH ist im Ergebnis zuzustimmen. Sofern der Access- bzw. Host-Provider einer gerichtlichen Anordnung zur

[161] EuGH GRUR 2012, 265, 267 (Rn. 38).
[162] EuGH GRUR 2012, 265, 267 (Rn. 39 f.).
[163] EuGH GRUR 2012, 265, 268 (Rn. 53).
[164] EuGH GRUR 2012, 265, 268 (Rn. 48).
[165] EuGH GRUR 2012, 265, 268 (Rn. 50 ff.).
[166] EuGH GRUR 2012, 382, 383 (Rn. 37).
[167] EuGH GRUR 2012, 382, 383 (Rn. 38).
[168] EuGH GRUR 2012, 382, 384 (Rn. 51).

Unterlassung nur in dem Sinne nachkommen kann, dass er hierfür umfangreiche Filtersysteme einzurichten hat, die jeglichen Datenverkehr überwachen, so verstößt dies gegen Art. 15 Abs. 1 ECRL. Denn durch die Einrichtung eines umfassenden Filtersystems, wäre der Host-Provider dazu gehalten, alle Inhalte der Nutzer unterschiedslos zu überwachen und zu prüfen. Eine solche pro-aktive Überwachung allgemeiner Art wollte der europäische Richtliniengeber gerade durch Art. 15 Abs. 1 ECRL ausschließen. Sofern der BGH sich in diversen Urteilen darauf beruft, dass die ISP gemäß Erwägungsgrund 48 der E-Commerce-Richtlinie die nach vernünftigen Ermessen von ihnen zu erwartenden in innerstaatlichen Rechtsvorschriften niedergelegten Sorgfaltspflichten anwenden müssen, um bestimmte Arten rechtswidriger Tätigkeiten aufzudecken oder zu verhindern[169], so kann dies nicht als Grundlage für eine umfassende Überwachungstätigkeit herangezogen werden.[170] Auch der EuGH scheint die in den Erwägungsgründen genannten Sorgfaltspflichten nicht entsprechend zu interpretieren, da er diese in keinem seiner Urteile erwähnt. Vielmehr ist nach der hier vertretenen Auffassung davon auszugehen, dass die Anwendung von Sorgfaltspflichten nicht mit dem allgemeinen Überwachungsverbot kollidieren darf. Solche Sorgfaltspflichten könnten vielmehr darin bestehen, den Nutzer in den AGB darauf zu verpflichten, dass er geistige Eigentumsrechte Dritter beachtet. Zudem ist in dem Erwägungsgrund die Rede von *bestimmten Arten* rechtswidriger Tätigkeiten. Dies könnte dahingehend ausgelegt werden, dass dem ISP nur hinsichtlich besonders schwerwiegender Delikte, wie bspw. Fälle von Kinderpornographie, gewisse Sorgfaltspflichten auferlegt werden können.[171] Eine Sorgfaltspflicht im Sinne einer

[169] Siehe bspw. BGH GRUR 2013, 1229, 1232 m.w.N.

[170] So ist auch *Marly* der Auffassung, dass sofern eine entsprechende Sorgfaltspflicht auf eine verbotene allgemeine Verpflichtung zur Überwachung fremder Informationen hinausliefe, der Erwägungsgrund 48 unberücksichtigt bleiben müsse, siehe Marly in Grabitz/Hilf, Band IV, ECRL Abschnitt 4, Art. 15 Rn. 7.

[171] So auch Marly in Grabitz/Hilf, Band IV, ECRL Abschnitt 4, Art. 15 Rn. 7.

allgemeinen Überwachung durch den ISP stünde jedenfalls im Widerspruch zu Art. 15 Abs. 1 ECRL und ist daher abzulehnen.[172]
Wünschenswert wären weitere Ausführungen gewesen, welche Maßnahmen im Lichte des Art. 15 Abs. 1 ECRL als zulässig zu erachten sind. Dass der EuGH hier allerdings keine differenzierteren Aussagen getroffen hat, ist der nicht sonderlich nuancierten Vorlagefrage des belgischen Gerichts geschuldet.
Wie sich im Laufe der Untersuchung zeigen wird, erlangt das Verbot einer allgemeinen Überwachungs- und Nachforschungspflicht insbesondere im Rahmen der Störerhaftung und etwaig geschuldeter Prüfpflichten große Bedeutung.[173]

bb) Verpflichtung zur Sperrung/Entfernung

Weiterhin bleiben nach § 7 Abs. 2 S. 2 TMG Verpflichtungen zur Entfernung und Sperrung der Nutzung von Informationen nach den allgemeinen Gesetzen auch im Falle der Nichtverantwortlichkeit des Diensteanbieters nach den §§ 8 bis 10 unberührt. Gebündelt umgesetzt wurden hiermit die Art. 12 Abs. 3, Art. 13 Abs. 2 und Art. 14 Abs. 2 ECRL.
So können gem. Art. 12 Abs. 3 und Art. 13 Abs. 2 ECRL die Mitgliedsstaaten Vorschriften festlegen, nach denen ein Gericht oder eine Verwaltungsbehörde vom Access- bzw. Cache-Provider verlangen kann, die Rechtsverletzung abzustellen oder zu verhindern. Zusätzlich zu dieser Bestimmung enthält der entsprechende Artikel für den Host-Provider in Art. 14 Abs. 3 ECRL den Zusatz, dass die Mitgliedsstaaten Verfahren für die Entfernung einer Information oder die Sperrung des Zugangs zu ihr festlegen können.
Der Zusatz der Entfernung bzw. Sperrung bei dem Host-Provider liegt offensichtlich darin begründet, dass diesen gem. Art. 14 Abs. 1 lit. b) ECRL die Verpflichtung zur Entfernung bzw. Sperrung nach Kenntnis einer Rechtsverletzung trifft, um eine Privilegierung in Anspruch nehmen zu können. Eine gleichartige Pflicht trifft den

[172] So auch in Grabitz/Hilf, Band IV, ECRL Abschnitt 4, Art. 15 Rn. 7.
[173] Siehe hierzu S. 134.

Access- oder den Cache-Provider nicht. Ihre Privilegierung ist insoweit umfassender als die des Host-Providers.

Der Verweis auf die Möglichkeit der Mitgliedstaaten, Verfahren für die Entfernung einer Information oder die Sperrung des Zugangs festlegen zu können, spiegelt die Möglichkeit der einzelnen Mitgliedstaaten wider, nationale *Notice and Takedown*-Regelungen festlegen zu können.[174] Von dieser Möglichkeit hat Deutschland allerdings keinen Gebrauch gemacht.[175] § 7 Abs. 2 TMG i.V.m. den jeweils einschlägigen Regelungen zur Haftungsfreistellung der verschiedenen ISP erlangt insbesondere Bedeutung im Rahmen der Störerhaftung und damit etwaig einhergehenden Prüfpflichten.[176]

Die entsprechende Bestimmung des TDG a.F. enthielt zudem die Beschränkung, dass die Sperrung technisch möglich und zumutbar sein muss. Auch wenn das TMG hierauf nicht mehr explizit abstellt, ist dennoch allgemein anerkannt, dass nichts verlangt werden kann, was unmöglich oder unzumutbar ist.[177]

§ 7 Abs. 2 TMG und dessen genaue Reichweite spielt daher insbesondere eine gewichtige Rolle, wenn es um die Frage der Zumutbarkeit von etwaig dem ISP aufzuerlegenden Maßnahmen geht.[178]

b) Host-Provider, § 10 TMG

Der Host-Provider ist gem. § 10 TMG für fremde Informationen, die er für einen Nutzer speichert, nicht verantwortlich, sofern er (1) keine Kenntnis von der rechtswidrigen Handlung oder der Information hat und ihm im Falle von Schadensersatzansprüchen auch keine Tatsachen oder Umstände bekannt sind, aus denen die rechtswidrige Handlung oder die Information offensichtlich wird, oder (2) unverzüglich tätig geworden ist, um die Information zu

---

[174] So auch Holznagel, S. 84; Siehe hierzu auch http://ec.europa.eu/internal_market/e-commerce/notice-and-action/index_en.htm, zuletzt besucht am 23.04.2016.

[175] Anders bspw. Finnland, Ungarn und Island, welche jeweils gesetzliche *Notice and Takedown*-Verfahren eingeführt haben, siehe hierzu Holznagel, S. 75 ff.

[176] Siehe hierzu S. 134, S. 152 und S. 163.

[177] BT-Drucksache 14/6098, S. 23.

[178] Siehe hierzu S. 66.

entfernen oder den Zugang zur ihr zu sperren, sobald er Kenntnis erlangt hat.

Bereits § 5 Abs. 2 TDG a.F. enthielt die Bestimmung, dass Host-Provider lediglich haften, wenn sie Kenntnis von den fraglichen Inhalten haben und es ihnen technisch möglich und zumutbar ist, deren Nutzung zu verhindern. Die Umsetzung der ECRL brachte damit zum einen eine Verschärfung hinsichtlich der Haftung im Rahmen von Schadensersatzansprüchen, befreit den Host-Provider aber gleichzeitig von einer Haftung, sofern er unverzüglich nach Kenntniserlangung tätig geworden ist.

aa) Personeller Anwendungsbereich

Dem Wortlaut nach kommt nur der Diensteanbieter, also der Host-Provider als natürliche oder juristische Person, in den Genuss der Haftungsprivilegien.[179] Damit würden die Mitarbeiter des Host-Providers automatisch aus dem Anwendungsbereich des § 10 TMG herausfallen. Da es jedoch in den meisten Fällen die Angestellten des Host-Providers sein werden, die Handlungen vornehmen, welche eine Haftung auslösen können, kommt es folglich zu einem Wertungswiderspruch.[180] Dieser ist nach h.M. durch „redaktionelle Berichtigung“ zu lösen, indem die Haftungsprivilegien auch auf Mitarbeiter zu erstrecken sind.[181]

bb) Fremde Informationen i.S.d. § 10 TMG

In Abänderung des § 5 TDG a.F. wurde durch die Umsetzung der ECRL der Begriff der „Inhalte“ durch den der „Informationen“ ersetzt. § 10 TMG wurde zudem sprachlich um die rechtswidrige Handlung ergänzt. Nach der Gesetzesbegründung sollte durch diese Ersetzung jedoch keine inhaltliche Änderung vorgenommen werden. Der neue Begriff der „Informationen“ sei gleichbedeutend mit dem der „Inhalte“ und umfasse demnach alle Angaben die vom

[179] Paal in BeckOK TMG, § 7 Rn. 21; Sieber/Höfinger in Hoeren/Sieber/Holznagel, Teil 18.1 Rn. 34.
[180] Sieber/Höfinger in Hoeren/Sieber/Holznagel, Teil 18.1 Rn. 34f.
[181] Paal in BeckOK InfoMedienR, § 7 TMG, Rn. 22; Sieber/Höfinger in Hoeren/Sieber/Holznagel, Teil 18.1 Rn. 35; Sieber, Rn. 258.

ISP übermittelt bzw. gespeichert werden.[182] Gemeint sind damit Daten aller Art, wie auch urheberrechtliche Werke, sofern sie elektronisch übermittelt werden.[183]

Die sprachliche Anpassung an die ECRL stellt insbesondere durch den Zusatz der rechtswidrigen Handlung klar, dass nicht nur inhaltliche Äußerungen, wie vereinzelt hinsichtlich des § 5 TDG a.F. angenommen wurde[184], hiervon umfasst sind, sondern auch an sich rechtmäßige Inhalte, deren Übermittlung lediglich rechtswidrig ist.[185] Ein klassischer Fall hierfür ist die illegale öffentliche Zugänglichmachung eines urheberrechtlich geschützten Werkes.

Um die Privilegierung in Anspruch nehmen zu können, muss es sich bei den fraglichen Informationen um fremde Informationen handeln. Nach Ansicht des BGH sind dies nach richtlinienkonformer Auslegung Informationen, die von dem Nutzer des Teledienstes eingegeben wurden und von denen der Host-Provider keine Kenntnis hat und über die er auch keine Kontrolle besitzt.[186]

Dass der deutsche Gesetzgeber in Abweichung zur ECRL den Begriff der „fremden" Informationen und damit eine Abgrenzung zu den in § 7 Abs. 1 TMG genannten „eigenen" Informationen vornimmt, wurde im Schrifttum oftmals kritisiert.[187] Da die Richtlinie von „durch einen Nutzer eingegebenen Informationen" spricht, wurde bezweifelt, dass zwischen den beiden Begriffen eine inhaltliche Kongruenz besteht. So indiziert der Wortlaut der ECRL eine auf den Akt der technischen Eingabe abstellende Interpretation.

Durch die Klarstellung des BGH, dass der Begriff „fremde Information" im Sinne des Art. 14 ECRL als von einem Nutzer

[182] BT-Drucks. 14/6098, S. 23.
[183] Altenhain in MüKo zum StGB, Vorbemerkung zu den §§ 7 ff., Rn. 14.
[184] OLG München, MMR 2001, 375, 376; Waldenberger, MMR 1998, 124, 127.
[185] So auch bereits vor der Umsetzung der ECRL: Waldenberger, MMR 1998, 378, 379.
[186] BGH GRUR 2014, 180, 181 – „Terminhinweis mit Kartenausschnitt".
[187] So z.B. Hoffmann in Spindler/Schuster, § 7 TMG, Rn. 14; Fitzner, GRUR Int 2012, 109, 113; Hoffmann, MMR 2002, 284, 288.

eingegebene Information zu verstehen ist, dürfte zumindest dieser Debatte weithin der Wind aus den Segeln genommen worden sein.
Noch immer umstritten ist hingegen das aus dem Begriff der eigenen Informationen gem. § 7 Abs. 1 TMG erschaffene Konzept der „zu eigen gemachten" Inhalte.

(1) Abgrenzung zu eigenen Informationen

Die Unterscheidung zwischen eigenen und fremden Informationen geht auf § 5 TDG a.F. zurück. § 5 Abs. 1 TDG a.F. enthielt den Grundsatz der Verantwortlichkeit für eigene Inhalte nach den allgemeinen Gesetzen, während § 5 Abs. 2 TDG a.F. die eingeschränkte Verantwortlichkeit für fremde Inhalte zum Gegenstand hatte.
Im Rahmen der Umsetzung der ECRL hat der deutsche Gesetzgeber an dieser Unterscheidung festgehalten.
Der in § 7 Abs. 1 TMG stipulierten Verantwortlichkeit des ISP für eigene Informationen kommt lediglich deklaratorische Wirkung zu.[188] Dass der ISP für eigene Inhalte die volle Verantwortung trägt ist selbsterklärend und fand aus diesem Grunde auch keinen Eingang in die ECRL.
Problematisch an der an sich redundanten Regelung des deutschen Rechts ist vor allem, dass aus § 7 Abs. 1 TMG eine Haftung für sog. „zu eigen gemachte" Informationen hergeleitet wird.[189] Denn hierdurch wird die Verantwortlichkeit der ISP auf Inhalte, welche ursprünglich nicht von den ISP sondern ihren Nutzern stammen, weiter ausgedehnt.

(2) Zu eigen gemachte Informationen

Bereits in der Gesetzesbegründung zum TDG a.F. hat der Gesetzgeber klargestellt, dass zu den eigenen Inhalten auch von Dritten hergestellte Inhalte zählen, welche sich der ISP zu eigen gemacht hat.[190] Diese Maxime übernimmt er sodann auch für das

[188] Altenhain in MüKo zum StGB, § 7 TMG, Rn. 2; Sieber/Höfinger in Hoeren/Sieber/Holznagel, Teil 18.1, Rn. 40.
[189] So auch Hoeren/Yankova, IIC 2012, 501, 528.
[190] BT-Drucks. 13/7385, S. 19.

TDG n.F. indem er ohne weitere inhaltliche Auseinandersetzung die Feststellung trifft, dass zu den eigenen Informationen nach § 8 TDG n.F. auch Informationen Dritter gehören, die sich der Diensteanbieter zu eigen macht.[191]

Im Schrifttum wird diesbezüglich die Frage nach der Vereinbarkeit dieses Konstrukts mit europäischen Vorgaben aufgeworfen.

Bereits hinsichtlich des TDG a.F. war die Figur des „zu eigen Machens" von fremden Inhalten, insbesondere deren Voraussetzungen, nicht unumstritten.[192]

(a) Rechtsprechung des BGH

Bereits mit Urteil vom 30.06.2009 hat der VI. Zivilsenat hinsichtlich des zu eigen Machens einer fremden Äußerung durch den Verpächter einer Domain Stellung genommen und festgestellt, dass es hierfür einer Identifizierung des Verbreiters mit der Äußerung derart bedarf, dass sie als seine eigene erscheint.[193] Bei der Bejahung einer solchen Identifikation sei grundsätzlich Zurückhaltung geboten.[194]

Bezüglich der Zurechnung von urheberrechtlich geschützten Inhalten als eigene Inhalte des Host-Providers entschied der I. Zivilsenat wenig später und konkretisierte die Anforderungen einer solchen.[195] Es komme für ein zu eigen Machen der Informationen auf die objektive Sicht auf der Grundlage einer Gesamtbetrachtung aller relevanten Umstände an.[196] Im streitgegenständlichen Fall hatte die Beklagte, eine Betreiberin einer Internetseite mit frei abrufbaren Rezepten, nach Ansicht des BGH tatsächlich und nach außen sichtbar die inhaltliche Verantwortung für die auf ihrer

[191] BT-Drucks. 14/6098, S. 23.
[192] Spindler, MMR 2004, 440, 441.
[193] BGH MMR 2009, 752, 753 – „Focus Online".
[194] BGH MMR 2009, 752, 753; Diese Beurteilung liegt auf einer Linie mit der früheren Rechtsprechung des erkennenden Senats aus dem Jahre 1976 hinsichtlich der Zurechnung einer ausgestrahlten Äußerung eines Dritten als eigene Äußerung der Fernsehanstalt – BGH GRUR 1976, 651, 653 – „Der Fall Bittenbinder".
[195] BGH MMR 2010, 556 – „marions-kochbuch.de".
[196] BGH MMR 2010, 556, 557.

Internetseite veröffentlichten Rezepte und dazugehörigen Fotos übernommen.[197]

Ausschlaggebend hierfür war zum einen, dass die Betreiberin der Internetseite die Bilder vorab einer redaktionellen Kontrolle unterwarf und diese somit nicht automatisch freigeschaltet wurden und zum anderen, dass die Rezepte inklusive Fotos mit dem Kochmützen-Emblem der Betreiberin versehen wurden.[198] Insofern sei auch unerheblich, dass der Nutzer der Plattform erkennen konnte, dass der als rechtsverletzend geltend gemachte Inhalt von einem Dritten stammt.[199]

Ferner spreche für ein zu eigen Machen der Inhalte, dass die Betreiberin der Internetseite sich umfassende Nutzungsrechte an den Inhalten von ihren Nutzern hat einräumen lassen und sie die Inhalte Dritten zur kommerziellen Nutzung anbietet.[200]

(b) Vereinbarkeit mit der ECRL

Die ECRL kennt keine Unterscheidung zwischen eigenen und fremden Informationen. Art. 14 ECRL spricht von „durch einen Nutzer eingegebenen Informationen“. Der europäische Richtliniengeber hat sich damit für einen technischen Ansatz entschieden, der darauf abstellt, wer die Information ursprünglich eingegeben hat und nicht inwiefern diese dem Host-Provider inhaltlich zugerechnet werden kann.

Im Schrifttum wird daher diese Differenzierung des deutschen Rechts zu Recht kritisiert.[201] Die Übernahme der Rechtsfigur aus Zeiten des TDG a.F. ist durch die europäischen Vorgaben der ECRL nicht mehr gedeckt.[202] Im Rahmen einer Vollharmonisierung bestimmt sich die Auslegung der deutschen Regelung des § 10 TMG nach der ECRL.[203] Dies hat auch der

[197] BGH MMR 2010, 556, 557.
[198] BGH MMR 2010, 556. 557.
[199] BGH MMR 2010, 556. 557.
[200] BGH MMR 2010, 556, 557.
[201] So bspw. Altenhain in MüKo zum StGB, Vorbemerkung zu den §§ 7 ff., Rn. 24; Fitzner, GRUR Int 2012, 109, 113; Hoeren/Yankova, IIC 2012, 501, 528; Sieber/Höfinger in Hoeren/Sieber/Holznagel, Teil 18.1, Rn. 39 ff.
[202] Fitzner, GRUR Int 2012, 109, 113; Hoeren/Yankova, IIC 2012, 501, 528.
[203] Sieber/Höfinger in Hoeren/Sieber/Holznagel, Teil 18.1, Rn. 39 ff.; Spindler,

BGH in seiner „Terminhinweis mit Kartenausschnitt"-Entscheidung bestätigt.[204] Mit Hinweis auf den Wortlaut des Art. 14 ECRL, „durch den Nutzer eingegebene Informationen", führte er aus, dass in diesem Sinne auch der Begriff der „fremden Informationen" gem. § 10 TMG auszulegen sei und der deutsche Gesetzgeber diesem Begriff keinen über Art. 14 ECRL hinausgehenden Inhalt geben durfte.[205]

Sofern allerdings zur Begründung des auf einem technischen Verständnis beruhenden Art. 14 ECRL auf Erwägungsgrund 42 der ECRL verwiesen wird[206], ist dies nicht überzeugend. Erwägungsgrund 42 bezieht sich eindeutig nur auf Access- und Cache-Provider und enthält keinerlei Aussagen hinsichtlich der Tätigkeit des Host-Providers. Dies wird zum einen aus dem Wortlaut deutlich. In Erwägungsgrund 42 ist lediglich die Rede von Diensteanbietern, die *„ein Kommunikationsnetzwerk [...] betreiben und den Zugang zu diesem [...] vermitteln, über das von Dritten zur Verfügung gestellte Informationen übermittelt oder zum alleinigen Zweck vorübergehend gespeichert werden, die Übermittlung effizienter zu gestalten"*. Damit verwendet der Europäische Richtliniengeber die Definition der Tätigkeit des Access- und Cache-Providers, wie sie in Art. 12 und 13 ECRL enthalten ist. Die Tätigkeit des Host-Providers, welche gem. Art. 14 ECRL darin besteht, vom Nutzer eingegebene Informationen zu speichern, wird hier nicht erwähnt.[207] Der hieran anknüpfende 43. und 44. Erwägungsgrund spricht deshalb auch von der „reinen Durchleitung" und „Caching". Erst der 46. Erwägungsgrund beschäftigt sich mit der Tätigkeit des Host-Providers.

MMR 2004, 440, 441.

[204] BGH GRUR 2014, 180, 181.

[205] BGH GRUR 2014, 180, 181.

[206] BGH GRUR 2014, 180, 181; Spindler, MMR 2004, 440, 441.

[207] Dieser Auffassung ist grundsätzlich auch Altenhain, welcher im Rahmen des § 10 Satz 2 in MüKo, § 10 TMG, Rn. 28 wie folgt ausführt: *„Laut Erwägungsgrund (42) decken die Art. 12, 13 ECRL nur Fälle eines automatischen Ablaufs ab, in denen der Diensteanbieter weder Kenntnis noch Kontrolle über die Information besitzt. Auch wenn dieser Erwägungsgrund nicht die dauerhafte Speicherung nach Art. 14 ECRL bzw. § 10 betrifft, ist ihm der grundsätzliche Gedanke einer Beschränkung auf technisch geprägte Sachverhalte mit mangelnder Kontroll- und Einflussmöglichkeit zu entnehmen."*

Neuere unterinstanzliche Rechtsprechung scheint zudem ein zu eigen Machen von Inhalten restriktiv auszulegen.[208]

(c) Rechtsprechung des EuGH – „aktive Rolle“

Auch wenn der Wortlaut der ECRL keinen Rückschluss auf eine Unterscheidung zwischen fremden und eigenen bzw. zu eigen gemachten Informationen zulässt, so hat der EuGH in zwei Entscheidungen den Anwendungsbereich des Art. 14 ECRL mit Hilfe eines anderen Konstrukts eingeschränkt.

In „Google France und Google“[209] führte er aus, dass die Speicherung eines Host-Providers nur dann unter Art. 14 ECRL fällt, sofern dessen Verhalten auf das eines „Vermittlers“ im Sinne der ECRL beschränkt ist.[210] Zur weiteren Erläuterung verweist der EuGH auf den 42. Erwägungsgrund der ECRL, wonach die Tätigkeit des Diensteanbieters *„rein technischer, automatischer und passiver Art“* ist, was bedeutet, dass er *„weder Kenntnis noch Kontrolle über die weitergeleitete oder gespeicherte Information besitzt“*.[211] Dabei verkennt der EuGH jedoch, wie zuvor erläutert, dass dieser Erwägungsgrund nicht den Host-Provider, sondern lediglich den Access- und Cache-Provider betrifft. Der hierin enthaltene Verweis auf „gespeicherte Information“ bezieht sich daher lediglich auf die vom Cache-Provider vorübergehend vorgenommene Speicherung.

Aus diesem Grunde beruht die hieran anknüpfende Prüfung bereits auf einem falschen Verständnis der Intention des Richtliniengebers. Der EuGH schlussfolgert hieraus, dass lediglich sofern der Host-Provider eine neutrale Rolle in der Erbringung seiner Dienste spiele, in dem Sinne, dass die Tätigkeit des Host-Providers rein

---

[208] So hat bspw. das OLG München im Fall der Videoplattform YouTube ausgeführt, dass selbst eine Kenntnis von den konkreten, durch die Nutzer vorgenommenen Verletzungshandlungen noch kein Zu-Eigen-Machen begründe, weil der maßgebliche verständige Durchschnittsnutzer daraus weder die Übernahme einer Verantwortung für die Inhalte noch eine Identifizierung mit diesen herleite, siehe OLG München, BeckRS 2016, 03388; ein zu eigen Machen von YouTube auch verneinend: OLG Hamburg, MMR 2016, 269.

[209] EuGH NJW 2010, 2029 – Urteil vom 23.03.2010, C-236/08 bis 238/08 „Google France und Google“.

[210] EuGH NJW 2010, 2029, 2035.

[211] EuGH NJW 2010, 2029, 2035.

technischer, automatischer und passiver Art ist und er weder Kenntnis noch Kontrolle über die weitergeleitete oder gespeicherte Information besitze, er durch Art. 14 ECRL privilegiert sei.[212] Sobald er eine aktive Rolle spiele, die ihm eine Kenntnis oder Kontrolle über die Informationen verschaffe, falle seine Privilegierung weg.[213]

Diese Unterscheidung zwischen neutralem und aktivem Host-Provider bestätigt der Gerichtshof in seiner „L'Oréal SA"-Entscheidung[214] und konkretisiert zugleich die Merkmale, durch die dem Host-Provider eine solche aktive Rolle zukommen kann. Wenn der Host-Provider Hilfestellung leiste, z.B. durch Optimierung der Präsentation der Verkaufsangebote sowie deren Bewerbung, könne davon ausgegangen werden, dass er eine aktive Rolle gespielt hat, die ihm eine Kenntnis oder Kontrolle der diese Angebote betreffenden Daten verschafft.[215] Bzgl. dieser Daten könne sich der Host-Provider nicht auf die Haftungsprivilegierung des Art. 14 ECRL berufen.[216]

Teilweise wird nach diesem Urteil die Meinung vertreten, dass durch die vom EuGH festgelegten Beurteilungsmaßstäbe kommerzielle Marktplätze aus dem Anwendungsbereich der ECRL vollständig herausfallen würden, da diese in der Regel gemäß der vom BGH gemachten Ausführungen Hilfestellung leisten würden.[217] *Hoeren*[218] ist daher der Auffassung, dass eine solche Beurteilung das Haftungsprivileg ad absurdum führt und weit über den Geist der ECRL hinausgeht.

Allerdings ist eine aktive Rolle nach dem Wortlaut des EuGH nicht schon alleine dann zu bejahen, wenn ein Host-Provider bspw. grundsätzlich einzelne Verkaufsangebote optimiert, sondern lediglich, wenn ihm eine solche Optimierung zusätzlich Kenntnis oder Kontrolle der solche Angebote betreffenden Daten

[212] EuGH NJW 2010, 2029, 2035.
[213] EuGH NJW 2010, 2029, 2035.
[214] EuGH MMR 2011, 596.
[215] EuGH MMR 2011, 596, 603.
[216] EuGH MMR 2011, 596, 603.
[217] Hoeren, MMR 2011, 605, 605.
[218] Hoeren, MMR 2011, 605, 605.

verschafft.[219] Dies bedeutet im Endeffekt also nicht mehr, als dass der entsprechende Host-Provider das spezifisch in Frage stehende Angebot durch Optimierungsmaßnahmen zur Kenntnis nehmen oder Einfluss darauf nehmen kann. Im Umkehrschluss heißt dies aber nicht, dass jegliche aktive Rolle des Host-Providers gleichzeitig seinen Ausschluss von den Privilegien rechtfertigt.

Zudem führt der Gerichtshof explizit aus, dass, sollte der Host-Provider sich entsprechend aktiv verhalten und Kontrolle oder Kenntnis über bestimmte Inhalte erhalten, der Host-Provider lediglich hinsichtlich dieser Daten seine Privilegierung verliert. Von einer grundsätzlichen Unanwendbarkeit der Privilegien auf diesen Host-Provider ist nicht die Rede.

Bei einer entsprechenden Bewertung sollte deshalb nicht nur die aktive Rolle des Host-Providers betrachtet werden, sondern im Anschluss die Frage gestellt werden, ob eine solche aktive Rolle ihm Kenntnis oder Kontrolle über bestimmte Inhalte verschafft. Erst dann ist im Lichte der EuGH Rechtsprechung die Anwendbarkeit der Privilegien auf diese spezifischen Inhalte ausgeschlossen.

Teilweise wird zudem im Schrifttum die Auffassung vertreten, dass die vom EuGH herausgearbeitete Unterscheidung zwischen aktivem und neutralem Anbieter das Pendant zum deutschen „zu eigen Machen“ darstellt.[220] In der Tat ist es so, dass beide richterlichen Konstrukte bei der Bewertung bestimmter Kriterien zu dem gleichen Ergebnis gelangen können.

Spindler gibt allerdings zu Bedenken, dass nach den bislang vom EuGH aufgestellten Kriterien die Hürde zur Annahme eines aktiven Host-Providers wesentlich niedriger sein dürfte als die für eine Qualifizierung eines „zu eigen gemachten“ Inhaltes.[221]

---

[219] BGH GRUR 2011, 1038, 1040; Wiebe, WRP 2012, 1182, 1187 f.
[220] Bergmann/Goldmann in Harte-Bavendamm/Henning-Bodewig, § 8 Rn. 134; Leistner, ZUM 2012, 722, 725; Spindler, MMR 2011, 703, 706.
[221] Spindler, MMR 2011, 703, 706.

(d) Ergebnis

Eine Einschränkung der Privilegien des Host-Providers durch die Erweiterung des Anwendungsbereichs des § 7 TMG ist aufgrund der zuvor genannten Gründe, insbesondere der Unvereinbarkeit mit EU-rechtlichen Vorgaben, nicht gerechtfertigt.

Die vom EuGH vorgenommene Unterscheidung zwischen aktivem und neutralem Provider beruht bereits auf einem falschen Verständnis des 42. Erwägungsgrundes der ECRL, welcher ausweislich lediglich für den Access- und Cache-Provider Geltung beansprucht.

Sieht man unabhängig von diesem falschen Verständnis der ECRL dennoch eine Nichtanwendbarkeit der Privilegien, sofern der Host-Provider durch seine aktiven Handlungen Kenntnis oder Kontrolle über spezifische Inhalte erlangt, so ist hier zwischen Kenntnis und Kontrolle zu unterscheiden. Sofern seine aktive Rolle dem Host-Provider Kenntnis der Inhalte verschafft, spiegelt dies letzten Endes nichts weiter wider als § 10 TMG, der den Host-Provider bei Kenntnis eines rechtswidrigen Inhalts und bei anschließender Untätigkeit ja auch von den Privilegien ausschließt.

Einzig unklar ist, wann eine Kontrolle des Host-Providers über die einzelnen Inhalte vorliegt. Hierzu hat der EuGH nicht weiter ausgeführt.

cc) Fehlende Kenntnis

Die Privilegierung des Host-Providers knüpft an das Vorliegen zweier alternativer Umstände. Dieser ist gem. § 10 S. 1 Nr. 1 TMG nicht verantwortlich, sofern er keine Kenntnis von der rechtswidrigen Handlung oder der Information hat und ihm im Falle von Schadensersatzansprüchen auch keine Tatsachen oder Umstände bekannt sind, aus denen die rechtswidrige Handlung oder die Information offensichtlich wird.

Entsprechend sind sowohl rechtsverletzende Verwertungshandlungen als auch an sich rechtsverletzende Informationen erfasst.[222]

(1) Kenntnis der rechtswidrigen Handlung oder der Information

Der Wortlaut dieser ersten Alternative wurde im Schrifttum oftmals kritisiert. Durch die Einfügung des Artikels „der“ vor „Information“ wird teilweise vertreten, dass das Attribut der Rechtswidrigkeit sich lediglich auf die Handlung beziehen würde, nicht jedoch auf die Information.[223] Entsprechend müsste bei der Frage der Kenntnis des Host-Providers bezüglich einer beanstandeten Handlung zudem die Frage gestellt werden, ob er Kenntnis von der Rechtswidrigkeit dieser Handlung hatte, während bei einer beanstandeten Information bereits die Kenntnis dieser Information an sich eine Kenntnis des Host-Providers begründen würde.

In der Praxis ergäbe sich hieraus das folgende Bild: Der Host-Provider erlangt, auf welchem Wege auch immer, Kenntnis über einen auf seiner Plattform hochgeladenen Film. Der Film an sich ist noch kein rechtswidriger Inhalt, von daher muss der Host-Provider zusätzlich Kenntnis darüber erlangen, dass er illegal, das heißt ohne Zustimmung des Rechtsinhabers, hochgeladen wurde, folglich eine rechtswidrige Handlung vorliegt.

Im Falle einer Information hingegen soll bereits die Kenntnis über diese Information die Kenntnis des Host-Providers begründen. Hintergrund hierfür soll sein, dass eine Kenntnis der Rechtswidrigkeit nicht erforderlich ist, da die Information an sich bereits die Rechtswidrigkeit ohne Weiteres offenbart.[224] Dies mag unproblematisch sein bei Informationen die an sich offensichtlich rechtswidrig sind, wie beispielsweise bei kinderpornographischen

[222] Soweit im Rahmen dieser Arbeit die Rede von rechtswidriger Information ist, umfasst dies auch immer die rechtswidrige Handlung.
[223] Sieber/Höfinger in Hoeren/Sieber/Holznagel, Teil 18.1 Rn. 88; Gercke, MMR 2003, 602, 603; Kartal-Aydemir/Krieg, MMR 2012, 647, 648; so auch BT-Drucks. 14/6098, S. 25.
[224] Kartal-Aydemir/Krieg, MMR 2012, 647, 648.

Inhalten. In weniger offensichtlichen Fällen ist diese Schlussfolgerung allerdings mehr als fraglich.

Altenhain folgert daher, dass das Merkmal der Rechtswidrigkeit sowohl im Zusammenhang mit der Handlung als auch mit der Information redundant ist.[225] Er begründet dies anhand einer Auslegung der ECRL. Zwar spreche Art. 14 ECRL von einer „Kenntnis von der rechtswidrigen Tätigkeit oder Information", damit würde aber keine zusätzliche Voraussetzung geschaffen.[226] Vielmehr würde durch die Tatsache, dass die ECRL keine konkreten Maßstäbe zur Beurteilung der Rechtswidrigkeit nennt, deutlich, dass durch den Zusatz der Rechtswidrigkeit lediglich verdeutlicht werden solle, um welche Art von Handlungen bzw. Informationen es bei der Privilegierung des Host-Providers gehe.[227] Denn ohne die Benennung entsprechender Maßstäbe zur Beurteilung der Rechtswidrigkeit, würde das jeweils national geltende Recht die Voraussetzungen der ECRL bestimmen, was dem Ziel der ECRL zuwiderlaufe, ein einheitliches, dem nationalen Recht vorgelagertes Haftungsregime zu schaffen.[228]

Dieser Argumentation kann nicht gefolgt werden. Bei der Frage der Rechtswidrigkeit geht es nicht um die Maßstäbe zur Beurteilung der Rechtmäßigkeit, sondern um die Frage, ob der Host-Provider von der Rechtswidrigkeit Kenntnis hatte. Ob und unter welchen Umständen eine spezifische Handlung oder Information als rechtswidrig anzusehen ist, ist prinzipiell nach dem jeweiligen nationalen Recht zu beurteilen. Dies spricht jedoch nicht gegen die durch die ECRL verfolgte Harmonisierung der Providerhaftung. Zudem wurde im Bereich des Urheberrechts ohnehin eine weitgehende multinationale bzw. europäische Harmonisierung der Verletzungstatbestände beispielsweise durch die Berner Übereinkunft[229], die InfoSoc-Richtlinie[230] und die Software-Richtlinie[231] hergestellt.

---

[225] Altenhain in MüKo zum StGB, § 10 TMG, Rn. 10.
[226] Altenhain in MüKo zum StGB, § 10 TMG, Rn. 10.
[227] Altenhain in MüKo zum StGB, § 10 TMG, Rn. 10.
[228] Altenhain in MüKo zum StGB, § 10 TMG, Rn. 10.
[229] Berner Übereinkunft zum Schutz von Werken der Literatur und Kunst

Es ist daher der herrschenden Meinung zuzustimmen, die davon ausgeht, dass die Kenntnis der Rechtswidrigkeit sowohl auf die Handlung als auch die Information bezogen werden muss.[232]

(2) Positive Kenntnis

Fraglich ist zudem, was genau unter dem Begriff der Kenntnis zu verstehen ist. Zur Bestimmung wurde bereits zum TDG a.F. auf bekannte Begrifflichkeiten aus dem Strafrecht zurückgegriffen. Die Begründung des Regierungsentwurfs zum TDG a.F. selbst spricht von einer Eingrenzung auf vorsätzliches Handeln gemäß der allgemeinen Grundsätze des Straf- und Ordnungswidrigkeitenrechts und einer entsprechenden unbedingten oder bedingten Kenntnis seitens des Host-Providers.[233] Diese Einbeziehung des bedingten Vorsatzes im Sinne des dolus eventualis stieß aber bereits zur alten Rechtslage im Schrifttum größtenteils auf Ablehnung.[234]

Der BGH schien sich dieser Meinung im Hinblick auf das TDG a.F. angeschlossen zu haben, indem er ausführte, dass Kenntnis des Host-Providers die positive Kenntnis des einzelnen, konkreten Inhaltes bedeute.[235] Da der Host-Provider folglich positiv wissen muss, dass eine Rechtsverletzung vorliegt, geht der BGH hier, ohne dies explizit zu benennen, von direktem Vorsatz im Sinne des dolus directus 1. oder 2. Grades aus. Der BGH fügt hinzu, dass jedenfalls ein „Kennenmüssen" nicht genüge.[236] Die Frage, ob demnach dolus eventualis zur Bejahung der Kenntnis ausreiche, hat der BGH

---

revidiert in Paris am 24. Juli 1971.

[230] Richtlinie 2001/29/EG des Europäischen Parlaments und des Rates vom 22. Mai 2001 zur Harmonisierung bestimmter Aspekte des Urheberrechts und der verwandten Schutzrechte in der Informationsgesellschaft.

[231] Richtlinie 2009/24/EG des Europäischen Parlaments und des Rates vom 23. April 2009 über den Rechtsschutz von Computerprogrammen.

[232] EuGH, MMR 2011, 596, 603; EuGH, NJW 2010, 2029, 2035; Hoffmann in Spindler/Schuster, § 10 TMG, Rn. 25; Müller-Broich, § 10 Rn. 4; Paal in BeckOK InfoMedienR, § 10 TMG, Rn. 29; Eck/Ruess, MMR 2003, 363, 365; Fitzner, GRUR Int 2012, 109, 113; Hoeren in Festschrift für Ulrich Eisenhardt, S. 243, 245.

[233] BT-Drucks. 13/7385, S. 20.

[234] Hoffmann in Spindler/Schuster, § 10 TMG Rn. 18; Sieber, MMR 1998, 438, 442; Spindler, MMR 2001, 737, 740; Spindler, NJW, 1997, 3193, 3196; Tettenborn, MMR 1999, 516, 519.

[235] BGH MMR 2004, 166, 167.

[236] BGH MMR 2004, 166, 167.

damit indirekt beantwortet. Unklar ist allerdings warum er zur Bekräftigung seiner Ausführungen Bezug auf die Gesetzgebungsmaterialien zum TDG a.F. nimmt, welche ja gerade dafür sprechen, den Eventualvorsatz einzubeziehen.

Bezüglich der Neufassung der Privilegien hat sich diese Definition der Kenntnis des BGH zum TDG a.F. für § 10 S. 1 Nr. 1 Hs. 1 TMG etabliert.[237] Dies entspricht auch dem Wortlaut der ECRL, welcher in Art. 14 von „tatsächlicher Kenntnis" spricht.

(3) Offensichtlichkeit/Umstandskenntnis

Umstritten sind die Voraussetzungen einer Kenntnis im Falle von Schadensersatzansprüchen. Laut Gesetz dürfen dem Host-Provider keine Tatsachen oder Umstände bekannt sein, aus denen die rechtswidrige Handlung oder Information offensichtlich wird.

Aus dieser Formulierung schließt die h.M., dass hier auch Fälle bewusster Fahrlässigkeit einbezogen werden, wodurch der Anwendungsbereich gegenüber den von dem 1. Halbsatz erfassten Ansprüchen folglich erweitert wird.[238]

Die m.M. hält an dem Erfordernis des Vorsatzes auch bei Schadensersatzansprüchen fest, schränkt den Anwendungsbereich aber dadurch ein, dass es hinsichtlich des Bewusstseins der Rechtswidrigkeit auf evidente Rechtsverletzungen ankomme.[239]

Der h.M. ist hier zu folgen. Dies bekräftigen auch die Gesetzgebungsmaterialien, in denen explizit aufgeführt wird, dass der Host-Provider bei Schadensersatzansprüchen auch bei „Kennenmüssen" haftet.[240]

Hiermit im Einklang steht die Rechtsprechung des EuGH. In seiner „L'Oréal"-Entscheidung hat der Gerichtshof ausgeführt, dass der Host-Provider sich im Rahmen von gegen ihn geltend gemachten

---

[237] Hoffmann in Spindler/Schuster, § 10 TMG Rn. 18; Müller-Broich, § 10 Rn. 4; Paal in BeckOK InfoMedienR, § 10 TMG, Rn. 24; Sieber/Höfinger in Hoeren/Sieber/Holznagel, Teil 18.1 Rn. 83; Fitzner, GRUR Int 2012, 109, 113; Hoeren in Festschrift für Ulrich Eisenhardt, S. 243, 245.

[238] Hoffmann in Spindler/Schuster, § 10 TMG, Rn. 38; Paal in BeckOK InfoMedienR, § 10 TMG, Rn. 33; Sieber/Höfinger in Hoeren/Sieber/Holznagel, Teil 18.1 Rn. 90; Müller-Broich, § 10 Rn. 5; Eck/Ruess, MMR 2003, 363, 364; Fitzner, GRUR Int 2012, 109, 113;

[239] Hoeren, MMR 2004, 166, 169.

[240] BT-Drucks. 14/6098, S. 22.

Schadensersatzansprüchen nicht auf eine Privilegierung berufen könne, wenn er sich etwaiger Tatsachen oder Umstände bewusst war, auf Grund derer ein sorgfältiger Wirtschaftsteilnehmer die Rechtswidrigkeit hätte feststellen müssen.[241] Das „Kennenmüssen" bezieht sich wie die tatsächliche Kenntnis auf die spezifische Rechtsverletzung, die geltend gemacht wird.[242]

(4) Bewusstes Wegschauen

Fraglich ist hingegen die Bewertung von grob fahrlässiger Unkenntnis des Host-Providers.

Die h.M. geht davon aus, dass streng genommen selbst bewusstes Wegschauen zu einer Haftungsprivilegierung des Host-Providers führt, da der Host-Provider hierdurch keine positive Kenntnis im Sinne des § 10 TMG besitzt.[243]

Um dem dadurch unerwünschten Ergebnis zu entgegnen, schlägt *Hoeren* vor, in Fällen, in denen der Host-Provider sich treuwidrig einer Kenntnisnahme verschließt, das bewusste Sichverschließen mit dem Grundgedanken von § 162 BGB einer Kenntnis gleichzustellen.[244] Danach gilt eine Bedingung als eingetreten, sofern die Partei, zu deren Nachteil der Eintritt der Bedingung gereichen würde, diesen wider Treu und Glauben verhindert. Fraglich ist jedoch, wie eine solche Rechtskonstruktion mit dem Ziel der ECRL, Rechtssicherheit für die Host-Provider zu schaffen, vereinbar ist. Diese Fiktion der Kenntnis könnte zudem mit den Vorgaben der ECRL unvereinbar sein, da hierdurch das durch die Richtlinie vorgegebene Merkmal der tatsächlichen Kenntnis verändert wird.

Es ist daher interessengerechter, das bewusste Augen-Verschließen vor einer rechtswidrigen Handlung oder Information der

---

[241] EuGH, MMR 2011, 596, 603.

[242] Siehe EuGH, MMR 2011, 596, 603: *„Da das Ausgangsverfahren zu einer Verurteilung zur Zahlung von Schadensersatz führen kann, ist [...] zu prüfen, ob eBay in Bezug auf die fraglichen Verkaufsangebote und insoweit, als diese L'Oréal-Marken verletzt haben, ‚sich etwaiger Tatsachen oder Umstände bewusst war, aus denen die rechtswidrige Tätigkeit offensichtlich wird'."*

[243] Hoffmann in Spindler/Schuster, § 10 TMG, Rn. 18; Paal in Beck InfoMedienR, § 10 TMG, Rn. 24; Hoeren in Festschrift für Ulrich Eisenhardt, S. 243, 245.

[244] Hoeren, MMR 2004, 672, 673.

Umstandskenntnis gleichzusetzen. Da dem bewussten Wegschauen des Host-Providers in der Regel ein Anfangsverdacht vorausgeht, könnte man hieraus schließen, dass dem Host-Provider ohne entsprechendes Wegschauen die Umstände bekannt geworden wären, aus denen die rechtswidrige Handlung bzw. Information offensichtlich geworden wäre. Er handelte somit mindestens bewusst grob fahrlässig.

(5) Vermutete Kenntnis - Gesetzentwurf zur Änderung des TMG

Bereits im Koalitionsvertrag der 18. Legislaturperiode hat die Bundesregierung festgehalten, dass sie die Rechtsdurchsetzung insbesondere gegenüber Plattformen verbessern will, deren Geschäftsmodell im Wesentlichen auf der Verletzung von Urheberrechten aufbaut.[245] Entsprechend sollen solche Diensteanbieter nicht länger das Haftungsprivileg für Host-Provider in Anspruch nehmen können und keine Werbeeinnahmen mehr erhalten.[246]

Ende 2015 hat die Bundesregierung einen Entwurf zur Änderung des TMG beschlossen, der das im Koalitionsvertrag Festgeschriebene umsetzen sollte (TMG-E).[247]

(a) Wortlaut der gesetzlichen Vermutung der Kenntnis

Nach dem Gesetzentwurf sollte § 10 TMG durch § 10 Abs. 2 TMG-E um folgenden Absatz ergänzt werden:

„Die Kenntnis von Tatsachen oder Umständen nach Absatz 1, aus denen die rechtswidrige Handlung oder die Information offensichtlich wird, wird vermutet, wenn es sich bei dem angebotenen Dienst um einen besonders gefahrgeneigten Dienst handelt. Ein besonders gefahrgeneigter Dienst liegt in der Regel dann vor, wenn

[245] Koalitionsvertrag zwischen CDU, CSU und SPD, S. 133.
[246] Koalitionsvertrag zwischen CDU, CSU und SPD, S. 133.
[247] Gesetzentwurf zur Änderung des TMG.

1. *die Speicherung oder Verwendung der weit überwiegenden Zahl der gespeicherten Informationen rechtswidrig erfolgt,*
2. *der Diensteanbieter durch eigene Maßnahmen vorsätzlich die Gefahr einer rechtsverletzenden Nutzung fördert,*
3. *in vom Diensteanbieter veranlassten Werbeauftritten mit der Nichtverfolgbarkeit bei Rechtsverstößen geworben wird oder*
4. *keine Möglichkeit besteht, rechtswidrige Inhalte durch den Berechtigten entfernen zu lassen.“*

(b) Begründung der gesetzlichen Vermutung der Kenntnis

Zur Begründung führte die Bundesregierung an, dass ein Vorgehen der Rechteinhaber gegen Diensteanbieter, deren Geschäftsmodell im Wesentlichen auf Rechtsverletzungen beruht, vielfach schwierig, wenn nicht unmöglich ist.[248] Da aber nach der allgemeinen Lebenserfahrung davon ausgegangen werden könne, dass dem Diensteanbieter bei solchen Diensten ausreichend viele Tatsachen oder Informationen bekannt sind, aus denen die rechtswidrige Handlung oder Information offensichtlich wird, wird eine gesetzliche Vermutung für eine Kenntnis solcher Dienste aufgestellt.[249]

Um für mehr Rechtsklarheit und Rechtssicherheit zu sorgen, zählt das Gesetz beispielhaft Fallkonstellationen auf, bei denen von einem besonders gefahrgeneigten Dienst ausgegangen werden kann.[250]

(c) Beschlussempfehlung des Deutschen Bundestags und Bewertung der gesetzlichen Vermutung der Kenntnis

Eine Änderung des § 10 TMG entsprechend dem Entwurf der Bundesregierung wurde vom Deutschen Bundestag Mitte 2016 gestrichen.[251] Der Bundestag wies darauf hin, dass die Kodifizierung eines einheitlichen Haftungsregimes für Rechtsverletzungen im Internet vorrangig eine europäische

[248] Gesetzentwurf zur Änderung des TMG, S. 16.
[249] Gesetzentwurf der Änderung des TMG, S. 15.
[250] Gesetzentwurf der Änderung des TMG, S. 15.
[251] BT-Drucks. 18/8645, S. 11.

Aufgabe sei und daher auch auf europäischer Ebene adressiert werden müsse.[252]

Die Streichung des Deutschen Bundestages ist zu begrüßen, da die geplante Änderung des § 10 TMG gegen unionsrechtliche Vorgaben verstoßen hätte.[253] Wie zuvor ausgeführt, werden durch § 10 S. 1 Nr. 1 Hs. 2 TMG Fälle von bewusster Fahrlässigkeit, also einer Kenntnis im Sinne des „Kennenmüssens" erfasst.[254] Der neue § 10 Abs. 2 TMG-E hingegen hätte diese Kenntnis anhand von Vermutungstatbeständen hinsichtlich eines gefahrgeneigten Dienstes fingiert. Damit hätte er die Tatbestandsvoraussetzung der Kenntnis erweitert und wäre über den durch Art. 14 ECRL gesteckten Rahmen der Privilegierungsvoraussetzungen hinausgegangen.[255] Dies hätte auch im Widerspruch gestanden zu der durch den EuGH vorgenommenen Konkretisierung zu der Frage, wann der Host-Provider sich Tatsachen oder Umstände bewusst ist, aus denen die rechtswidrige Tätigkeit oder Information offensichtlich wird. Danach verliert der Host-Provider seine Privilegierung, wenn er sich etwaiger Tatsachen oder Umstände bewusst war, auf deren Grundlage ein sorgfältiger Wirtschaftsteilnehmer die in Rede stehende Rechtswidrigkeit hätte feststellen müssen.[256]

Der Gesetzesentwurf hätte folglich eine Haftungsverschärfung für den Host-Provider dargestellt, welche nicht im Einklang mit der durch die ECRL intendierte Vollharmonisierung gestanden hätte.[257] Zudem ist zu bezweifeln, dass durch die Gesetzänderung die von der Regierung selbst formulierten Ziele erreichen worden wären. Vielmehr hätte die Änderung des § 10 TMG zu weniger Rechtsklarheit geführt und damit auch weniger Rechtssicherheit für die Host-Provider, insbesondere durch die Einführung weiterer

[252] BT-Drucks. 18/8645, S. 11.
[253] So auch Frey/Rudolph/Oster, Gutachten, S. 30; Bitkom, Stellungnahme zur Änderung des TMG, S. 5 ff.
[254] Siehe S. 53.
[255] Frey/Rudolph/Oster, Gutachten, S. 35.
[256] EuGH MMR 2011, 596, 603.
[257] Bitkom, Stellungnahme zur Änderung des TMG, S. 5.

unbestimmter Rechtsbegriffe, wie dem des „besonders gefahrgeneigten Dienstes“.

dd) Wissenszurechnung

Nicht erforderlich ist, dass der Host-Provider selbst bzw. bei juristischen Personen dessen gesetzlicher Vertreter Kenntnis von der rechtswidrigen Information hat.[258] Wie bereits unter C.I.3 ausgeführt, ist Adressat der §§ 7 ff. TMG nicht lediglich das Unternehmen selbst bzw. dessen Inhaber, sondern auch die Mitarbeiter die für das Unternehmen in Ausübung der ihnen übertragenen Aufgaben tätig werden. Dem Diensteanbieter ist daher regelmäßig die Kenntnis seiner Mitarbeiter zuzurechnen.[259] Umstritten ist die rechtliche Grundlage für eine solche Wissenszurechnung. Ein Teil des Schrifttums rekurriert auf die allgemeinen zivilrechtlichen Zurechnungsregeln und die Heranziehung des Rechtsgedankens des § 166 Abs. 1 BGB und rechnet entsprechend dem Host-Provider das Wissen seiner Mitarbeiter zu, sofern der Mitarbeiter die Kenntnis im Rahmen der ihm betrauten Arbeitsaufgabe erhält.[260] Richtigerweise ist hinsichtlich der Anforderungen der Wissenszurechnung jedoch nicht auf nationale Zurechnungsmaßstäbe zurückzugreifen, sondern das nationale Recht soweit wie möglich am Wortlaut und Zweck der Richtlinie auszurichten, um den mit der Richtlinie, auf der das nationale Recht beruht, verfolgten Zweck zu erreichen.[261] Da ohne Erstreckung der Kenntnis auf die Mitarbeiter des Host-Providers die Bestimmung des § 10 TMG größtenteils ins Leere laufen würde, ist in richtlinienkonformer Auslegung dem Host-Provider

[258] Altenhain in MüKo zum StGB, § 10 TMG, Rn. 17; Hoffmann in Spindler/Schuster, § 10 TMG, Rn. 27; Paal in BeckOK InfoMedienR, § 10 TMG, Rn. 25.
[259] Altenhain in MüKo zum StGB, § 10 TMG, Rn. 17; Hoffmann in Spindler/Schuster, § 10 TMG, Rn. 27; Paal in BeckOK InfoMedienR, § 10 TMG, Rn. 25.
[260] Hoffmann in Spindler/Schuster, § 10 TMG, Rn. 27 f.; Paal in BeckOK InfoMedienR, § 10 TMG, Rn. 25.
[261] Walter/Obwexer in von der Groeben/Schwarze/Hatje, EUV Artikel 4, Rn. 116.

als Unternehmen auch die Kenntnis seiner Mitarbeiter zuzurechnen.[262]

Mit der gleichen Begründung sind auch die Stimmen im Schrifttum zurückzuweisen, die diese Wissenszurechnung für den Bereich des Strafrechts mit der Begründung ablehnen, dass dort die individuelle Schuld festgestellt werden müsse.[263] Eine unterschiedliche Behandlung ist bereits aufgrund der Funktion der Privilegien als Vorfilter sowie deren horizontaler Geltung verfehlt.[264] So steht es dem strafrechtlichen Grundsatz der individuellen Schuld keineswegs entgegen, auf der ersten Stufe der Prüfung im Rahmen des § 10 TMG eine Wissenszurechnung zu bejahen, um dann im zweiten Schritt der Prüfung eine strafrechtliche Verantwortlichkeit gerade aufgrund dieses Merkmals entfallen zu lassen. *Altenhain* weist in diesem Zusammenhang richtigerweise daraufhin, dass im Rahmen des zweiten Prüfungsschritts nach strafrechtlichen Maßstäben bei Fahrlässigkeitsdelikten die Kenntnis des Mitarbeiters durchaus eine Rolle spielen kann, bspw. für die Frage ob der Host-Provider dadurch fahrlässig gehandelt hat, dass er es unterlassen hat, seine Mitarbeiter dahingehend anzuweisen, Kenntnis über rechtsverletzende Inhalte mitzuteilen.[265]

ee) Unverzügliches Tätigwerden nach Kenntniserlangung

Für den Fall, dass der Host-Provider Kenntnis von der Rechtsverletzung erlangt, ist er gem. § 10 S. 1 Nr. 2 TMG noch immer privilegiert, sofern er unverzüglich tätig geworden ist, um die Information zu entfernen oder den Zugang zu ihr zu sperren.

Unerheblich ist, auf welchem Weg der Host-Provider die Kenntnis erlangt hat.[266] Denkbar sind sowohl Hinweise von Rechteinhabern, Hinweise Dritter oder aber auch die Wahrnehmung durch den Host-Provider selbst, wobei sich bei letzterem die Frage nach der Möglichkeit einer Beweisführung stellt.

---

[262] Altenhain in MüKo zum StGB, § 10 TMG, Rn. 19.
[263] So bspw. Hoffmann in Spindler/Schuster, § 10 TMG, Rn. 29.
[264] So auch Altenhain in MüKo zum StGB, § 10 TMG, Rn. 17.
[265] Altenhain in MüKo zum StGB, § 10 TMG, Rn. 17.
[266] Altenhain in MüKo zum StGB, § 10 TMG, Rn. 12; Paal in BeckOK InfoMedienR, § 10 TMG, Rn. 40.

Fraglich ist, wann von einem unverzüglichen Handeln ausgegangen werden kann. Die Richtlinie enthält keine Definition und keine starre Zeitgrenze hinsichtlich des Merkmals der Unverzüglichkeit. Es erscheint gerechtfertigt, das Merkmal in Anlehnung an die für den nationalen Bereich des Privatrechts geltende Definition des § 121 Abs. 1 S. 1 BGB auszulegen und ein unverzügliches Tätigwerden des Host-Providers dann anzunehmen, sofern dieser ohne schuldhaftes Zögern handelt.[267] Zur Bestimmung des genauen Zeitrahmens kommt es jeweils auf die konkreten Umstände des Einzelfalls an, insbesondere auf die Offensichtlichkeit der Rechtsverletzung und einer damit etwaig zusammenhängenden, notwendigen rechtlichen Prüfung seitens des Host-Providers.[268] Eine allgemeingültige Angabe eines angemessenen Zeitrahmens ist nicht möglich und auch nicht geboten.[269]

Ein Tätigwerden seitens des Host-Providers in Form der Entfernung oder Sperrung des Inhalts hat, auch ohne explizite Erwähnung im Gesetz, im Rahmen des technisch Möglichen und Zumutbaren zu erfolgen.[270] Entsprechend ist auch der Eintritt des Erfolgs keine Voraussetzung für eine Privilegierung des Host-Providers.[271] Das Löschen oder Sperren einzelner Inhalte auf dem Server des Host-Providers dürfte in der Regel jedoch ohne Probleme möglich sein.[272]

---

[267] Altenhain in MüKo zum StGB, § 10 TMG, Rn. 26; Hoffmann in Spindler/Schuster, § 10 TMG, Rn. 46.

[268] Hoffmann in Spindler/Schuster, § 10 TMG, Rn. 46; Paal in BeckOK InfoMedienR, § 10 TMG, Rn. 46.

[269] So aber Krüger Apel, MMR 2012, 144, 145, welche davon ausgehen, dass bei eindeutig unzulässigen Inhalten ein Tätigwerden des Host-Provider innerhalb von 24 Stunden zu erfolgen hat, bei einer vorherigen rechtlichen Prüfung müsse diese innerhalb einer Woche abgeschlossen sein.

[270] Altenhain in MüKo zum StGB, § 10 TMG, Rn. 25; Hoffmann in Spindler/Schuster, § 10 TMG, Rn. 44; Paal in BeckOK InfoMedienR, § 10 TMG, Rn. 43.

[271] Altenhain in MüKo zum StGB, § 10 TMG, Rn. 24; Hoffmann in Spindler/Schuster, § 10 TMG, Rn. 44; Paal in BeckOK InfoMedienR, § 10 TMG, Rn. 42.

[272] Altenhain in MüKo zum StGB, § 10 TMG, Rn. 25.

ff) Kein Unterordnungs- bzw. Beaufsichtigungsverhältnis

Gem. § 10 S. 2 TMG ist der Host-Provider von der Privilegierung ausgeschlossen, sofern der Nutzer dem Diensteanbieter untersteht oder von ihm beaufsichtigt wird.

Weder die Gesetzgebungsmaterialien zum TMG noch zur ECRL enthalten genauere Ausführungen zur Bedeutung dieser Vorschrift.

Es ist nach dem Wortlaut davon auszugehen, dass ein „Unterstehen" immer gegeben ist, wenn der Nutzer dem Host-Provider in grundsätzlicher und längerfristiger Art und Weise untersteht, beispielsweise im Rahmen eines Über- und Unterordnungsverhältnisses zwischen Arbeitnehmer und Arbeitgeber.[273] Allerdings dürften hiervon grundsätzlich keine Fälle erfasst sein, in denen der Arbeitnehmer im Rahmen seiner zugewiesenen Tätigkeit für den Arbeitgeber handelt, da die in diesem Fall gespeicherten Informationen eigene des Arbeitgebers darstellen.[274] Fraglich ist auch, wie die Speicherung von Informationen durch den Arbeitnehmer einzuordnen ist, wenn dieser außerhalb der ihm zugewiesenen Tätigkeit gehandelt hat, also privat die Infrastruktur des Arbeitgebers nutzt. Da es nach dem Wortlaut grundsätzlich auf das Verhältnis zwischen Host-Provider und Nutzer ankommt und nicht darauf, ob dieser konkreten Einfluss auf die Speicherung durch den Nutzer hat, ist auch in diesem Fall davon auszugehen, dass § 10 S. 2 TMG greift.[275]

Eine „Beaufsichtigung" hingegen dürfte sich auf eine konkrete Situation oder Tätigkeit beziehen, in welcher der Host-Provider eine Aufsichtspflicht gegenüber dem Nutzer hat, beispielsweise die Schule gegenüber ihren Schülern.[276]

In der Praxis scheint dieses Merkmal jedoch keine sonderliche Rolle zu spielen.

---

[273] Altenhain in MüKo zum StGB, § 10 TMG, Rn. 28; Hoffmann in Spindler/Schuster, § 10 TMG, Rn. 48.

[274] Altenhain in MüKo zum StGB, § 10 TMG, Rn. 29; Hoffmann in Spindler/Schuster, § 10 TMG, Rn. 50.

[275] A.A. Altenhain in MüKo zum StGB, § 10 TMG, Rn. 29; Hoffmann in Spindler/Schuster, § 10 TMG, Rn. 50.

[276] Hoffmann in Spindler/Schuster, § 10 TMG, Rn. 50; Paal in BeckOK InfoMedienR, § 10 TMG, Rn. 54.

gg) Anwendbarkeit auf Unterlassungsansprüche

Von mit Abstand größter Brisanz ist die Frage der Anwendbarkeit des Host-Provider-Privilegs auf die deutsche Störerhaftung und damit auf Unterlassungsansprüche.

(1) Frühe Rechtsprechung des BGH

In dem Fall Internetversteigerung I[277] beschäftigte sich der I. Zivilsenat des BGH mit der Verantwortlichkeit der Hosting-Plattform eBay für Markenrechtsverletzungen, hier der Marke „Rolex", die durch einen Nutzer begangen wurden.

Mit Urteil vom 11.03.2004 führte der BGH bezüglich der Unanwendbarkeit der §§ 7 ff. TMG auf Unterlassungsansprüche wie folgt aus:

„Wie sich aus dem Gesamtzusammenhang der gesetzlichen Regelung ergibt, findet die Haftungsprivilegierung des § 11 TDG n.F. indessen keine Anwendung auf Unterlassungsansprüche."[278]

Da der Host-Provider die Rechtsverletzung jedoch nicht selbst vorgenommen hat, sondern lediglich als Störer haftet, setzt seine Haftung auf Unterlassung die Verletzung von zumutbaren Prüfpflichten voraus.[279] Dem Host-Provider sei nicht zuzumuten, jedes Angebot vor Veröffentlichung auf Rechtsverletzungen zu untersuchen, er müsse allerdings, sofern er auf eine klare Rechtsverletzung hingewiesen wurde, nicht nur die konkrete Rechtsverletzung unverzüglich sperren, sondern auch Vorsorge dafür treffen, durch entsprechende Prüf- und Filterverfahren, dass es nicht zu weiteren derartigen Markenverletzungen kommt.[280]

Zudem wäre der Host-Provider für einen Verstoß gegen das Unterlassungsgebot nur haftbar zu machen, sofern ihn ein Verschulden im Sinne des § 890 ZPO trifft.[281]

---

[277] BGH MMR 2004, 668.
[278] BGH MMR 2004, 668, 670.
[279] BGH MMR 2004, 668, 671.
[280] BGH MMR 2004, 668, 671 f.
[281] BGH MMR 2004, 668, 672.

Zur inhaltlichen Begründung stützt der BGH sich auf folgende Argumente:

(a) Wortlaut

Der Wortlaut des § 11 Satz 1 TDG n.F. spreche von der „Verantwortlichkeit“ des Diensteanbieters.[282] Damit werde lediglich die strafrechtliche Verantwortlichkeit und die Schadensersatzhaftung adressiert.[283]

(b) § 8 Abs. 2 TDG a.F./Art. 14 Abs. 3 ECRL

Dass Unterlassungsansprüche nicht von den Privilegien erfasst seien, würde auch durch § 8 Abs. 2 TDG n.F. nahe gelegt, der besagt, dass „Verpflichtungen zur Entfernung oder Sperrung der Nutzung von Informationen nach den allgemeinen Gesetzen [...] auch im Falle der Nichtverantwortlichkeit des Diensteanbieters nach den §§ 9 bis 11 unberührt (bleiben)“.[284]

§ 8 Abs. 2 TDG n.F. decke sich insoweit mit Art. 14 Abs. 3 ECRL, der deutlich mache, dass Unterlassungsansprüche von dem Privileg eben nicht erfasst seien.[285] Demnach lässt Art. 14 ECRL *„die Möglichkeit unberührt, dass ein Gericht oder eine Verwaltungsbehörde nach den Rechtssystemen der Mitgliedsstaaten vom Diensteanbieter verlangt, die Rechtsverletzung abzustellen oder zu verhindern, oder dass die Mitgliedsstaaten Verfahren für die Entfernung einer Information oder die Sperrung des Zugang zu ihr festlegen.“*

Diese Ansicht werde zudem durch den 46. Erwägungsgrund gestützt.[286]

(c) Schadensersatzanspruch v. Unterlassungsanspruch

Auch ließe sich nur durch die Nichtanwendung der Privilegien auf Unterlassungsansprüche erklären, warum an Schadensersatzansprüche geringere Anforderungen gestellt werden

[282] BGH MMR 2004, 668, 670.
[283] BGH MMR 2004, 668, 670.
[284] BGH MMR 2004, 668, 670.
[285] BGH MMR 2004, 668, 670.
[286] BGH MMR 2004, 668, 670.

als für die Verantwortlichkeit i.Ü.[287] Wären Unterlassungsansprüche von § 11 Satz 1 Nr. 1 Alt. 1 TDG n.F. erfasst, so hätte dies zur Folge, dass an den Unterlassungsanspruch höhere Anforderungen gestellt werden als an den Schadensersatzanspruch.[288]

(d) § 5 Abs. 4 TDG a.F.

Zu guter Letzt seien Unterlassungsansprüche bereits von § 5 Abs. 4 TDG a.F. nicht erfasst worden.[289] Die Gesetzesbegründung zum TDG a.F. führte hierzu explizit aus, dass Verpflichtungen zur Unterlassung, die keine Schuld voraussetzen, von den Privilegien unberührt bleiben sollen.[290]

(e) Vorbeugende Unterlassungsansprüche

In dem Urteil Internetversteigerung II ging der BGH noch einen Schritt weiter und urteilte, dass das Haftungsprivileg des § 10 S. 1 TMG auch auf vorbeugende Unterlassungsansprüche nicht anwendbar sei.[291] Der Host-Provider als Störer könne demnach vorbeugend auf Unterlassung in Anspruch genommen werden, auch wenn es noch zu keiner Rechtsverletzung gekommen sei, sondern lediglich eine Erstbegehungsgefahr begründet sei.[292] Es müsse bei einer drohenden Gefährdung nicht erst abgewartet werden, bis es tatsächlich zu einer Rechtsverletzung kommt.[293]

(f) Zwischenergebnis

Im Ergebnis hafte die Plattform daher als Störerin auf Unterlassung, da sie nach Hinweis auf die konkrete Rechtsverletzung nicht nur das konkrete Angebot hätte sperren müssen, sondern auch entsprechende Vorsorge hätte tragen müssen, durch technisch mögliche und zumutbare Maßnahmen,

[287] BGH MMR 2004, 668, 670.
[288] BGH MMR 2004, 668, 670.
[289] BGH MMR 2004, 668, 670.
[290] BT-Drucks. 13/7385, S. 21.
[291] BGH MMR 2007, 507, 508.
[292] BGH MMR 2007, 507, 510.
[293] BGH MMR 2007, 507, 510.

dass es nicht zu weiteren derartigen Markenrechtsverletzungen kommt.[294]

Mit dieser Rechtsprechung auf einer Linie stehen die in den darauffolgenden Jahren ergangenen Entscheidungen des I. Zivilsenats Internetversteigerung II[295], Jugendgefährdende Medien bei eBay[296], Internetversteigerung III[297] und marions-kochbuch.de[298] sowie die des VI. Zivilsenats Meinungsforum[299], spickmich.de[300] und Focus Online[301].

(2) Bewertung der früheren Rechtsprechung des BGH

Die Rechtsprechung des BGH erfuhr auch im Schrifttum erhebliche Kritik.[302]

Sie ist unter zwei verschiedenen Aspekten fragwürdig. Zum einen ist die prinzipielle Nichtanwendbarkeit der Privilegien auf Unterlassungsansprüche nicht durch die europäischen Vorgaben gerechtfertigt, zum anderen konstruiert der BGH durch die Störerhaftung und damit einhergehenden Prüfpflicht eine zusätzliche Voraussetzung, welche der Host-Provider nach Kenntnis einer Rechtsverletzung zu erfüllen hat, um in den Genuss der Privilegierung zu kommen.

Die Argumente, welche der BGH zur Rechtfertigung der Nichtanwendung des § 10 TMG auf Unterlassungsansprüche anführt, können größtenteils problemlos entkräftet werden.

---

[294] BGH MMR 2004, 668, 672.

[295] BGH MMR 2007, 507, in welcher der BGH die Unanwendbarkeit der Haftungsprivilegien auf vorbeugende Unterlassungsansprüche ausdehnt, sofern eine entsprechende Erstbegehungsgefahr begründet ist.

[296] BGHZ 173, 188 = GRUR 2007, 890, wobei der BGH hier für den Bereich des Wettbewerbsrecht auf eine täterschaftliche Haftung aufgrund einer Verletzung der wettbewerbsrechtlichen Verkehrspflicht abstellt und nicht auf eine Haftung als Störer.

[297] BGH GRUR 2008, 702.

[298] BGH MMR 2010, 556.

[299] BGH GRUR 2007, 724.

[300] BGHZ 183, 328 = MMR 2009, 608.

[301] BGH MMR 2009, 752.

[302] Frey/Rudolph, Rechtsgutachten zur Evaluierung des Haftungsregimes für Host- und Access-Provider im Bereich der Telemedien, S. 115; Hoeren, MMR 2004, 672, 672; Leible/Sosnitza, NJW 2004, 3225, 3226; Sobola/Kohl, CR 2005, 443, 449.

(a) Wortlaut-Argument

Der Begriff der Verantwortlichkeit in Art. 11 TDG a.F. beruht auf der europäischen Vorgabe des Art. 14 ECRL.

Bei der Auslegung einer gemeinschaftsrechtlichen Vorschrift ist zunächst dem Umstand Rechnung zu tragen, dass die Vorschriften in mehreren Sprachen abgefasst sind, so dass diese verschiedenen Fassungen gleichermaßen herangezogen werden müssen.[303] Zudem hat das Gemeinschaftsrecht eine eigene, besondere Terminologie, so dass eine Auslegung des Begriffs nach nationaler Dogmatik nicht geboten ist.[304] Im Übrigen ist jede Vorschrift des Gemeinschaftsrechts in ihrem Zusammenhang und im Lichte der jeweiligen Zielsetzung auszulegen.[305]

Die ECRL enthält keine Definition des Begriffs der Verantwortlichkeit.

In der englischen Fassung ist jedoch beispielsweise die Rede von „liable". Und der Begriff der „liability", den man am besten als Haftung übersetzt, setzt eben kein wie auch immer geartetes Verschulden voraus.[306]

Zudem wird der Begriff der Verantwortlichkeit auch im allgemeinen Zivilrecht für die verschuldensunabhängige Haftung gebraucht, so z.B. in § 645 BGB (Verantwortlichkeit des Bestellers) oder § 287 Abs. 2 BGB (Verantwortlichkeit während des Verzugs). Die Argumentation des BGH bezüglich des Begriffs der Verantwortlichkeit ist daher nicht überzeugend.[307]

(b) § 8 Abs. 2 TDG n.F./Art. 14 Abs. 3 ECRL

Auch die Bezugnahme auf die Bestimmung des § 8 Abs. 2 TDG n.F., wonach Verpflichtungen zur Entfernung oder Sperrung der Information nach den allgemeinen Gesetzen im Falle der

[303] EuGH, NJW 1983, 1257, 1258.
[304] EuGH, NJW 1983, 1257, 1258.
[305] EuGH, NJW 1983, 1257, 1258.
[306] Vgl. auch Sieber/Höfinger in Hoeren/Sieber/Holznagel, Teil 18.1, Rn. 15; Hoeren in Festschrift für Ulrich Eisenhardt, S. 243, 250.
[307] So auch Frey/Rudolph, Rechtsgutachten zur Evaluierung des Haftungsregimes für Host- und Access-Provider im Bereich der Telemedien, S. 102.

Nichtverantwortlichkeit des Diensteanbieters nach den §§ 9 bis 11 TDG n.F. unberührt bleiben, ist nicht überzeugend.

Wie der BGH korrekt ausführt, hat der deutsche Gesetzgeber mit dieser Vorschrift Art. 14 Abs. 3 ECRL umgesetzt, welcher besagt, dass ein Gericht oder eine Verwaltungsbehörde nach den Rechtssystemen der Mitgliedstaaten vom Diensteanbieter verlangen kann, die Rechtsverletzung abzustellen oder zu verhindern, oder dass die Mitgliedstaaten Verfahren für die Entfernung einer Information oder die Sperrung des Zugangs zu ihr festlegen.

Nach der Systematik und dem Wortlaut der deutschen und europäischen Bestimmung sind von der Privilegierung des Host-Providers auch Unterlassungsansprüche erfasst („im Falle der Nichtverantwortlichkeit nach den §§ 9 bis 11 TDG n.F."; „Dieser Artikel lässt die Möglichkeit unberührt, [...]"). Unabhängig von dieser Privilegierung können den Host-Provider aber bestimmte Verpflichtungen treffen.[308] Diese Verpflichtungen spiegeln sich entsprechend in § 10 S. 1 Nr. 2 TMG wider, welcher bei Kenntnis eben eine Entfernung bzw. Sperrung durch den Host-Provider verlangt, sofern dieser weiterhin eine Privilegierung in Anspruch nehmen will.[309]

Die gesamte Systematik des § 7 Abs. 2 S. 2 TMG in Verbindung mit § 10 S. 1 Nr. 2 TMG spricht daher gerade dafür, dass auch der verschuldensunabhängige Unterlassungsanspruch grundsätzlich von den Haftungsprivilegien erfasst wird.[310] Um dem Erfordernis des § 10 S. 1 Nr. 2 TMG gerecht zu werden, sind die Entfernung oder Sperrung eines Inhaltes jedoch grundsätzlich zulässig.[311]

Hiervon zeugt auch die Stellung der europäischen Regelung innerhalb des Art. 14 ECRL. Aus der Entscheidung des deutschen

---

[308] Vgl. auch Hoeren in Festschrift für Ulrich Eisenhardt, S. 243, 253.
[309] Vgl. auch Hoeren in Festschrift für Ulrich Eisenhardt, S. 243, 250.
[310] So auch Frey/Rudolph, Rechtsgutachten zur Evaluierung des Haftungsregimes für Host- und Access-Provider im Bereich der Telemedien, S. 104.
[311] So auch Frey/Rudolph, Rechtsgutachten zur Evaluierung des Haftungsregimes für Host- und Access-Provider im Bereich der Telemedien, S. 104.

Gesetzgebers die Verpflichtung zur Entfernung bzw. Sperrung vor die speziellen Verantwortlichkeitsregelungen der §§ 8-10 TMG zu stellen kann nicht geschlossen werden, dass Unterlassungsansprüche generell aus dem Anwendungsbereich der Privilegien heraus fallen.[312]

Die in Art. 14 Abs. 3 ECRL genannten „Verfahren für die Entfernung einer Information oder die Sperrung des Zugangs zu ihr" betreffen mögliche nationale *Notice and Takedown*-Verfahren, welche die Mitgliedstaaten zur Umsetzung des Art. 14 Abs. 1 lit. b) ECRL festlegen können.

(c) Schadensersatzanspruch v. Unterlassungsanspruch

Nach Auffassung des BGH hätte die Anwendbarkeit der Privilegien die schwer verständliche Folge, dass an den Unterlassungsanspruch höhere Anforderungen gestellt werden würden als an den Schadensersatzanspruch.[313]

Dieser scheinbare Widerspruch lässt sich allerdings mit einem Blick auf Art. 14 Abs. 1 lit. b) ECRL auflösen, welcher eine Pflicht zur Entfernung bzw. Sperrung bereits bei Umstandskenntnis auslöst, um etwaigen Schadensersatzansprüchen nach Art. 14 Abs. 1 lit. a) ECRL zu entgehen.[314] Dass der deutsche Gesetzgeber hier die europäischen Vorgaben nur ungenau umgesetzt hat und sich in § 10 S. 1 Nr. 2 TMG lediglich auf „diese Kenntnis" bezieht, ist insoweit unbeachtlich und im Lichte der europäischen Bestimmung so auszulegen, dass hier sowohl die tatsächliche Kenntnis als auch das Bewusstsein einer Rechtsverletzung erfasst werden.

Im Umkehrschluss bedeutet dies, dass der Host-Provider faktisch auch bereits in Fällen von Kennenmüssen die entsprechenden Informationen entfernen bzw. den Zugang zu ihnen sperren muss, um weiterhin in den Genuss der Privilegierung zu kommen. Hat der

[312] Paal in BeckOK InfoMedienR, § 7 TMG, Rn. 54.
[313] BGH MMR 2004, 668, 670.
[314] So im Ergebnis auch Sieber/Höfinger in Hoeren/Sieber/Holznagel, Teil 18.1, Rn. 51; Gersdorf/Paal in BeckOK InfoMedienR, § 7 TMG, Rn. 59 insoweit aber unrichtig, als dass sie für den Unterlassungsanspruch eine Umstandskenntnis ausreichen lassen wollen.

Host-Provider diese Verpflichtung erfüllt, ist er auch gegenüber weitergehenden Unterlassungsansprüchen privilegiert.

(d) § 5 Abs. 4 TDG a.F.

Zur Rechtfertigung seiner Rechtsprechung bezüglich der Unanwendbarkeit der Privilegien auf Unterlassungsansprüche verweist der BGH schließlich auf § 5 Abs. 4 TDG a.F. Auch dies vermag nicht zu überzeugen. Zunächst war auch bezüglich dieser alten Regelung bereits nicht unumstritten, ob diese Unterlassungsansprüche erfasste.[315] Die Beantwortung dieser Frage kann letzten Endes aber offen bleiben, da sie jedenfalls für die Auslegung der neuen Regelungen des TMG, welche auf den Vorgaben der ECRL basieren, unbeachtlich ist. Daher ist auch der Rückgriff des BGH auf die Begründung des Gesetzesentwurfs zum TDG a.F.[316] nicht geboten.[317]

Zur historischen Auslegung hätte der BGH vielmehr auf die Gesetzgebungsmaterialien zur ECRL sowie zum EGG zurückgreifen müssen.

(e) Vorbeugende Unterlassungsansprüche

Auch die Entscheidung hinsichtlich der Unanwendbarkeit der Haftungsprivilegien auf vorbeugende Unterlassungsansprüche ist abzulehnen und erfuhr sogar unter den Befürwortern der Unanwendbarkeit auf Unterlassungsansprüche erheblichen Gegenwind.

So führt *Spindler*[318] in seiner Urteils-Anmerkung zu Internetversteigerung II aus, dass die Störerhaftung nach Kenntnisnahme noch damit begründet werden könne, dass in diesem Fall nur spezifische Überwachungspflichten greifen würden, es sich bei der vorbeugenden jedoch nicht mehr um eine spezifische Überwachungspflicht handeln würde.

---

[315] Siehe bspw. Hoeren in Festschrift für Ulrich Eisenhardt, S. 243, 252 m.w.N.
[316] BT-Drucks. 13/3785, S. 21.
[317] So auch Frey/Rudolph, Rechtsgutachten zur Evaluierung des Haftungsregimes für Host- und Access-Provider im Bereich der Telemedien, S. 105.
[318] Spindler, MMR 2007, 511, 512.

(f) Zwischenergebnis

Die Argumentation des BGH bezüglich der Unanwendbarkeit der Haftungsprivilegien auf Unterlassungsansprüche ist aus den zuvor genannten Gründen nicht überzeugend.

Zudem steht sie im Widerspruch zu § 7 Abs. 2 S. 1 TMG, durch den Art. 15 Abs. 1 ECRL umgesetzt wurde. Demnach sind Diensteanbieter nicht verpflichtet, die von ihnen übermittelten oder gespeicherten Informationen zu überwachen oder nach Umständen zu forschen, die auf eine rechtswidrige Tätigkeit hinweisen.

Wenn den Host-Provider nun aber nach Kenntnis über eine spezifische Rechtsverletzung einer Prüfpflicht unterliegt und diese sich darauf bezieht, dass er Vorsorge treffen muss, dass es nicht zu weiteren kerngleichen Rechtsverletzungen kommt, dann kommt dies faktisch einer allgemeinen Überwachungspflicht des Host-Providers seines Dienstes gleich. Um dafür zu sorgen, dass die von der Prüfpflicht betroffenen Inhalte künftig nicht auf seiner Plattform erscheinen, hat er entsprechende Maßnahmen zu ergreifen. In der Praxis bedeutet dies, dass er sämtliche Inhalte der Nutzer vorab überprüfen muss. Nur so kann er im Bereich des technisch Möglichen und Zumutbaren sicherstellen, dass er nicht als Störer auf Unterlassung haftet.

Dies gilt umso mehr, da der BGH diese Pflicht nicht nur auf Material bezieht, welches durch den ursprünglichen Rechtsverletzer auf seine Plattform geladen wurde, sondern auch durch andere Nutzer auf die Plattform geladen wurde.[319]

Nach Auffassung des BGH sei dem Host-Provider in dieser Hinsicht zuzumuten, sich einer Filtersoftware zu bedienen, welche durch die Eingabe bestimmter Suchbegriffe Verdachtsfälle aufdeckt und die ermittelten Treffer gegebenenfalls anschließend einer manuellen Nachkontrolle zu unterziehen.[320]

Von den Befürwortern einer entsprechenden Prüfpflicht wird angeführt, dass es sich in diesen Fällen nicht um eine allgemeine Überwachungsverpflichtung im Sinne des § 7 Abs. 2 S. 1 TMG

[319] BGH GRUR 2007, 890, 894.
[320] BGH MMR 2007, 507, 511.

handele sondern um eine Überwachungspflicht im spezifischen Fall.[321]

Dem wird allerdings zu Recht entgegengehalten, dass eine Verpflichtung zur Filterung sämtlicher übermittelter Informationen, selbst wenn diese ursprünglich auf einer spezifischen Rechtsverletzung basiert, letzten Endes eine allgemeine Überwachungspflicht darstellt, da hierdurch alle Informationen vorbeugend kontrolliert werden müssen.[322] Der Host-Provider ist verpflichtet, die von den Nutzern gespeicherten Informationen zu überwachen, um diejenigen Fälle herausfiltern zu können, bezüglich derer ihn eine entsprechende Prüfpflicht trifft. Denn um seiner Prüfpflicht nachzukommen, reicht es für den Host-Provider nicht aus, lediglich bestimmte Informationen oder Rechtsverletzer zu überwachen. Er hat dafür Sorge zu tragen, dass die bereits als rechtsverletzend beanstandeten Inhalte nicht mehr auf seiner Plattform zugänglich gemacht werden. Dies bedeutet, dass durch entsprechend programmierte Filterprogramme, soweit dies technisch möglich ist, bestimmte Inhalte vorab herausgefiltert werden müssen. Da unklar ist, ob und durch welche Nutzer nochmals entsprechend rechtsverletzende Inhalte eingestellt werden, hat der Host-Provider sämtliche Inhalte zu filtern und ggf. manuell zu überprüfen.

Die Koppelung der Störerhaftung an die Verletzung von Prüfpflichten bürdet dem Host-Provider zudem eine zusätzliche Voraussetzung auf, die er für die Inanspruchnahme der Privilegien erfüllen muss.

Aus den zuvor genannten Gründen hätte die Frage, ob die vom BGH vertretene Ansicht hinsichtlich Unterlassungsansprüchen mit der ECRL vereinbar ist, dem EuGH vorgelegt werden müssen.[323]

(3) EuGH-Urteil L'Oréal

Im Jahr 2011 hatte auch der EuGH Gelegenheit, sich mit der ECRL und deren Voraussetzungen auseinanderzusetzen.

[321] Spindler, MMR 2007, 511, 512.
[322] Sieber/Höfinger in Hoeren/Sieber/Holznagel, Teil 18.1, Rn. 54.
[323] So auch Spindler, MMR 2007, 511, 512.

Gegenstand des Verfahrens war die Frage der Verantwortlichkeit des Betreibers eines Online-Marktplatzes für Markenrechtsverletzungen seiner Nutzer sowie die Möglichkeit gerichtliche Anordnungen gegen diesen, auch im Falle einer Nichtverantwortlichkeit, zu erwirken.

Der EuGH beschäftigte sich in der sog. „L'Oréal"-Entscheidung[324] konkret mit den folgenden zwei Fragen.

Zunächst wollte das vorlegende Gericht, der High Court of Justice, wissen, ob die vom Betreiber eines Online-Marktplatzes erbrachte Dienstleistung unter Art. 14 Abs. 1 ECRL fällt und, falls die Frage bejaht wird, unter welchen Voraussetzungen davon auszugehen ist, dass der Betreiber des Online-Marktplatzes Kenntnis i.S.v. Art. 14 Abs. 1 ECRL hat.[325]

Zudem wollte das Gericht wissen, ob Art. 11 Durchsetzungs-RL von den Mitgliedsstaaten verlangt, den Inhabern von Rechten geistigen Eigentums die Möglichkeit einzuräumen, dem Host-Provider gerichtliche Anordnungen erteilen zu lassen, mit denen diesem aufgegeben wird, Maßnahmen zu ergreifen, um künftigen Rechtsverletzungen vorzubeugen und, falls diese Frage bejaht wird, welche Anordnungen dies sein könnten.

Der EuGH beantwortete die erste Frage dahingehend, dass Art. 14 ECRL Anwendung auf den Betreiber einer Online-Plattform findet, sofern dieser keine aktive Rolle gespielt hat, die ihm Kenntnis oder Kontrolle über die gespeicherten Inhalte ermöglicht hat.[326] Im Falle von Schadensersatzansprüchen kann der Host-Provider sich nicht auf die Privilegierung des Art. 14 ECRL berufen, sofern er sich etwaiger Tatsachen oder Umstände bewusst war, auf deren Grundlage ein sorgfältiger Wirtschaftsteilnehmer die Rechtswidrigkeit der Inhalte hätte feststellen müssen und er in diesem Fall nicht unverzüglich tätig geworden ist.[327]

[324] EuGH, MMR 2011, 596.
[325] EuGH, MMR 2011, 596, 602.
[326] EuGH, MMR 2011, 596, 603.
[327] EuGH, MMR 2011, 596, 603.

Hinsichtlich der zweiten Vorlagefrage urteilte der EuGH, dass Art. 11 S. 3 Durchsetzungs-RL von den Mitgliedsstaaten verlangt, sicherzustellen, dass die nationalen Gerichte dem Host-Provider aufgeben können, Maßnahmen zu ergreifen, die nicht nur zur Beendigung der Rechtsverletzung, sondern auch zur Vorbeugung gegen erneute derartige Verletzungen beitragen.[328] Diese Maßnahmen müssen wirksam, verhältnismäßig und abschreckend sein und dürfen keine Schranken für den rechtmäßigen Handel errichten.[329]

(4) Bewertung L'Oréal-Urteil

Es ist fraglich, ob den Ausführungen des EuGH überhaupt Erkenntnisse hinsichtlich der deutschen Störerhaftung bzw. einer entsprechenden Unanwendbarkeit der Privilegien auf Unterlassungsansprüche entnommen werden können.

Während ein Teil des Schrifttums das Urteil als Bestätigung der deutschen Störerhaftung anpreist[330], geht ein anderer Teil davon aus, dass der EuGH diese Frage überhaupt nicht thematisiert hat[331].

In der Tat hat der EuGH diese Problematik nicht direkt angesprochen, allerdings lassen sich aus den Urteilsgründen einige Rückschlüsse für die Auslegung des deutschen Rechts ziehen.

Zunächst führt der Gerichtshof aus, dass grundsätzlich die Voraussetzungen für die Feststellung einer Verantwortlichkeit des Host-Providers dem jeweiligen nationalen Recht zu entnehmen sind.[332] Allerdings schreiben die Art. 12 bis 15 ECRL bestimmte Fälle vor, in denen, gegebenenfalls entgegen der einschlägigen nationalen Bestimmung, eben keine Verantwortlichkeit festgestellt werden darf.[333]

In der Folge geht der EuGH auf die Verantwortlichkeitsprivilegierung des Art. 14 Abs. 1 ECRL ein

[328] EuGH, MMR 2011, 596, 605.
[329] EuGH, MMR 2011, 596, 605.
[330] So bspw. Ensthaler/Heinemann, GRUR 2012, 433, 436; Leistner, ZUM 2012, 722, 736; Spindler, MMR 2011, 703, 706.
[331] Backhaus, LMK 2011, 326132; Hoeren, MMR 2011, 605, 605.
[332] EuGH, MMR 2011, 596, 602 (Rn. 107).
[333] EuGH, MMR 2011, 596, 602 (Rn. 107).

und erläutert, dass in Fällen, in denen der Diensteanbieter unter Art. 14 Abs. 1 ECRL fällt, dieser von jeder Verantwortlichkeit für die von ihm gespeicherten, rechtswidrigen Inhalte freigestellt ist, sofern er keine Kenntnis hiervon hatte.[334] Dem gewählten Wortlaut des Gerichtshofs nach gilt die Privilegierung demnach für jegliche Verantwortlichkeit, eine Unterscheidung zwischen strafrechtlicher, verschuldensabhängiger oder verschuldensunabhängiger Verantwortlichkeit nimmt er nicht vor.

Im Gegenteil, im Rahmen der Prüfung der zweiten Vorlagefrage, beschäftigt sich der EuGH gerade mit dem Umfang gerichtlicher Anordnungen gegenüber dem Host-Provider, worunter auch Anordnungen auf Unterlassung fallen.

In diesem Zusammenhang führt der Gerichtshof aus, dass dem Host-Provider gem. Art. 11 S. 3 Durchsetzungs-RL Maßnahmen aufgegeben werden könnten, die nicht nur zur Beendigung der Rechtsverletzung, sondern auch wirksam zur Vorbeugung gegen erneute Verletzungen beitragen.[335] Diese Auslegung werde auch gestützt durch Art. 18 ECRL, nach der die Mitgliedsstaaten Maßnahmen ermöglichen müssen, um eine mutmaßliche Rechtsverletzung abzustellen oder zu verhindern, dass den Betroffenen weiterer Schaden entsteht.[336]

In Anbetracht des Art. 15 Abs. 1 ECRL i.V.m. Art. 2 Abs. 3 Durchsetzungs-RL dürften Maßnahmen allerdings nicht darin bestehen, aktiv alle Kunden zu überwachen. Dies würde auch dem Erfordernis der Gerechtigkeit, Verhältnismäßigkeit und nicht übermäßiger Kosten, die Art. 3 Durchsetzungs-RL fordert, nicht gerecht werden.[337]

Zudem dürfe die Anordnung gegen den Host-Provider kein allgemeines und dauerhaftes Verbot zum Gegenstand haben oder bewirken können, auf der Plattform solche Waren anzubieten, die Gegenstand der Markenrechtsverletzung waren.[338]

---

[334] EuGH, MMR 2011, 596, 603 (Rn. 119).
[335] EuGH, MMR 2011, 596, 604 (Rn. 131).
[336] EuGH, MMR 2011, 596, 604 (Rn. 132).
[337] EuGH, MMR 2011, 596, 604 (Rn. 139).
[338] EuGH, MMR 2011, 596, 604 (Rn. 140).

In der Folge listet der EuGH Anordnungen auf, welche, trotz der zuvor genannten Beschränkungen sowohl als wirksam als auch verhältnismäßig anzusehen sind. Hierunter fällt zum einen der Ausschluss des Verletzers, um somit zu vermeiden, dass erneute derartige Rechtsverletzungen derselben Marke durch denselben Händler auftreten.[339] Zudem sind Maßnahmen denkbar, die eine Identifizierung der Händler erleichtern.[340]

Der Gerichtshof geht folglich mit keinem Wort auf die vom BGH konstruierte Pflicht ein, im Rahmen der Störerhaftung durch besondere Prüfungs- und Überwachungsmaßnahmen zu verhindern, dass es nicht zu weiteren kerngleichen Rechtsverletzungen kommt. Er hätte die Möglichkeit nutzen können, diese Verpflichtung hier klar zu benennen, hat darauf aber verzichtet und stattdessen beispielhaft Maßnahmen genannt, welche dem Host-Provider durch gerichtliche Anordnung auferlegt werden können, nämlich zum Ausschluss des Rechtsverletzers sowie zu dessen Identifizierung, um hierdurch zu verhindern, dass es zu erneuten, derartigen Verletzungen kommt.

Die Ausführungen des EuGH lassen jedoch großen Interpretationsspielraum zu bei der Frage, welche Maßnahmen dem Host-Provider im Rahmen des Art. 11 S. 3 Durchsetzungs-RL, dessen Pendant im Bereich des Urheberrechts Art. 8 Abs. 3 InfoSoc-RL darstellt, auferlegt werden dürfen, ohne hierdurch den allgemeinen Grundsatz des Art. 15 Abs. 1 ECRL zu berühren.

Dass der EuGH bei der Auslegung des Art. 14 ECRL keine Unterscheidung zwischen einer Haftung auf Schadensersatz und einer Haftung auf Unterlassung vornimmt, spricht jedenfalls eindeutig für die grundsätzliche Anwendbarkeit der Privilegien auf sämtliche Verantwortlichkeitsbereiche, was somit auch verschuldensunabhängige Ansprüche mit einschließt.[341]

---

[339] EuGH, MMR 2011, 596, 604 f. (Rn. 141).
[340] EuGH, MMR 2011, 596, 605 (Rn. 142).
[341] So auch Ohly, ZUM 2015, 308, 312; von Ungern-Sternberg, GRUR 2012, 321, 327; Wiebe, WRP 2012, 1182, 1186.

(5) Weiterentwicklung der Rechtsprechung des BGH

Nach der „L'Oréal"-Entscheidung des EuGH sahen einige Stimmen in Literatur und Rechtsprechung die bisherigen Ausführungen des BGH zur Störerhaftung als unvereinbar mit den europäischen Vorgaben.[342] Grund hierfür ist, dass der EuGH in seiner Rechtsprechung bei der Auslegung der europäischen Vorschriften zur Haftungsprivilegierung nicht zwischen Schadensersatz- oder Unterlassungsansprüchen unterscheidet und die Privilegien auch auf Unterlassungsansprüche anwendet.[343]

Entsprechend wurden auch die nachfolgenden BGH-Entscheidungen „Stiftparfum"[344], „Alone in the Dark"[345] und „Kinderhochstühle II"[346] teilweise als Abkehr von der bisherigen Leitlinie bezüglich der Anwendbarkeit der Privilegien auf Unterlassungsansprüche verstanden.[347]

So führt der BGH in seiner „Stiftparfum"-Entscheidung aus, dass es dem Host-Provider grundsätzlich nicht zuzumuten sei, alle Inhalte vor Veröffentlichung auf mögliche Rechtsverletzungen hin zu untersuchen.[348] Wurde er allerdings auf eine klare Rechtsverletzung hingewiesen und erlangt dadurch die gem. § 10 TMG erforderliche Kenntnis, trifft ihn die durch einen Unterlassungsanspruch durchsetzbare Verpflichtung, zukünftige derartige Verletzungen zu verhindern.[349] Im Gegensatz zu früheren Urteilen nimmt der BGH damit explizit Bezug auf die Privilegien und knüpft die Kenntnis einer Rechtsverletzung, die Prüfpflichten bei ihm ausgelöst, an eine Kenntnis i.S.d. § 10 TMG.

---

[342] KG, ZUM 2013, 886, 889; Köhler in Köhler/Bornkamm, § 8 UWG, Rn. 2.28; Hacker, GRUR-Prax 2011, 391, 393; Ohly, ZUM 2015, 308, 312; Ohly, GRUR 2010, 776, 784, welche durch die Google France-Entscheidung bereits bezweifelt, dass die vom BGH aufgestellten Grundsätze mit EU-Recht vereinbar sind; von Ungern-Sternberg, GRUR 2012, 321, 327.

[343] KG, ZUM 2013, 886, 889; Hacker, GRUR-Prax 2011, 391, 393; Ohly, ZUM 2015, 308, 312.

[344] BGHZ 191, 19 = GRUR 2011, 1038.

[345] BGHZ 194, 339 = MMR 2013, 185.

[346] BGH MMR 2014, 55.

[347] OLG Hamburg, MMR 2016, 269, 271; OLG Köln, GRUR 2014, 1081, 1089; Hacker, GRUR-Prax 2011, 391, 393; Lorenz, jurisPR-ITR 6/2012 Anm. 4.

[348] BGH GRUR 2011, 1038, 1040.

[349] BGH GRUR 2011, 1038, 1040; siehe in der Folge auch BGH MMR 2014, 55, 57; BGH MMR 2013, 185, 187.

In seiner Urteilsbegründung bezieht sich der I. Zivilsenat zudem auf die vom EuGH in seinem „L'Oréal"-Urteil aufgestellten Maßstäbe. Demnach sei der Host-Provider grundsätzlich gem. Art. 14 Abs. 1 ECRL für fremde Informationen nicht verantwortlich sowie gem. Art. 15 Abs. 1 ECRL auch nicht verpflichtet, die von ihm gespeicherten Informationen zu überwachen oder nach Umständen zu forschen, die auf eine rechtswidrige Tätigkeit hinweisen.[350]

Art. 11 S. 3 der Durchsetzungs-RL verlange jedoch, dass die Mitgliedsstaaten sicherstellen, dass die für den Schutz der geistigen Eigentumsrechte zuständigen nationalen Gerichte dem Host-Provider Maßnahmen auferlegen können, die nicht nur zu einer Beendigung der maßgeblichen Rechtsverletzung sondern auch zur Vorbeugung gegen erneute derartige Rechtsverletzungen beitragen.[351]

(6) Bewertung der Weiterentwicklung der Rechtsprechung des BGH

Auch wenn der BGH dies nicht expliziert thematisiert hat, ist das „Stiftparfum"-Urteil als eine zumindest teilweise Abkehr von seiner bisherigen Rechtsprechung zu werten, die allerdings kaum praktische Auswirkungen hat.

Ein Indiz hierfür ist zum einen, dass der Gerichthof nicht mehr, wie in seinen Urteilen zuvor, zunächst auf die grundsätzliche Unanwendbarkeit der Privilegien auf Unterlassungsansprüche eingeht. Vielmehr erläutert er die vom EuGH in der „L'Oréal"-Entscheidung aufgestellten Maßstäbe, nach denen der Host-Provider grundsätzlich gem. Art. 14 ECRL, dessen Regelung durch § 10 TMG in deutsches Recht umgesetzt wurde, nicht für Rechtsverletzungen seiner Nutzer verantwortlich ist, dass er jedoch nach Kenntnis unverzüglich tätig werden muss, um die

[350] BGH GRUR 2011, 1038, 1040.
[351] BGH GRUR 2011, 1038, 1040.

Informationen zu entfernen bzw. den Zugang zu ihnen zu sperren.[352]

Der Host-Provider sei lediglich dann nicht von dem Anwendungsbereich des Art. 14 ECRL erfasst, sofern er seine neutrale Vermittlerposition verlasse und eine aktive Rolle spiele, welche ihm Kenntnis oder Kontrolle über die Inhalte verschafft.[353]

Zusammenfassend stellt der BGH demnach fest, dass

„nach den Grundsätzen des Gerichtshofs und des erkennenden Senats [...] der Betreiber eines Online-Marktplatzes mithin verantwortlich [ist, Anmerkung des Verfassers], sobald er Kenntnis von einer Rechtsverletzung durch ein auf dem Marktplatz eingestelltes Verkaufsangebot erlangt. Ihn trifft weiter die durch einen Unterlassungsanspruch durchsetzbare Verpflichtung, zukünftige derartige Verletzungen zu verhindern.“[354]

Deshalb sei es auch für die für den Unterlassungsanspruch erforderliche Wiederholungsgefahr erforderlich, dass es nach Kenntnis einer bestimmten Rechtsverletzung zu einer vollendeten weiteren Verletzung kommt.[355] Die Verletzungshandlung, welche Gegenstand der Abmahnung war, könne keine Wiederholungsgefahr begründen.[356]

Durch die explizite Bezugnahme auf § 10 TMG im Rahmen der Kenntniserlangung des Host-Providers wendet der BGH die Haftungsprivilegien auch auf den Bereich der Unterlassungsansprüche an.[357]

Allerdings hält er weiterhin an einer Prüfpflicht im Rahmen der Störerhaftung nach erstmaliger Kenntnis einer Rechtsverletzung fest. Somit wird der Host-Provider nicht, wie § 10 S. 1 Nr. 2 TMG

[352] BGH GRUR 2011, 1038, 1040.
[353] BGH GRUR 2011, 1038, 1040.
[354] BGH GRUR 2011, 1038, 1040.
[355] BGH GRUR 2011, 1038, 1042.
[356] BGH GRUR 2011, 1038, 1042.
[357] BGH MMR 2014, 55, 57; BGH MMR 2013, 185, 186; A.A. Frey, MMR 2016, 275, 276, der die Bezugnahme auf § 10 TMG lediglich als erforderlich im Rahmen der Prüfung des Verbots der allgemeinen Überwachungspflichten gem. § 7 Abs. 2 S. 1 TMG ansieht.

vorschreibt, privilegiert, sofern er unverzüglich nach Kenntnis die Information entfernt oder den Zugang sperrt, sondern seine anschließende Privilegierung wird an ein zusätzliches Kriterium geknüpft.

(7) Ergebnis

Nach der aktuellen Rechtsprechung des BGH ist davon auszugehen, dass dieser auch Unterlassungsansprüche der grundsätzlichen Anwendbarkeit des § 10 TMG unterwerfen will.[358] Allerdings lässt die bisherige Rechtsprechung aufgrund der weiterhin auferlegten Prüfpflichten eine konsequente Anwendung der Privilegien bislang vermissen.

Demnach ist der Host-Provider im Rahmen des § 10 S. 1 Nr. 1 TMG privilegiert, sofern er keine Kenntnis hat. Erhält er aber Kenntnis über eine Rechtsverletzung gem. § 10 S. 1 Nr. 1 TMG, so hat er diese unverzüglich gem. § 10 S. 1 Nr. 2 TMG zu entfernen bzw. den Zugang zu ihr zu sperren. Es bestehen für den Host-Provider gem. § 7 Abs. 2 S. 1 TMG grundsätzlich keine Verpflichtungen die Inhalte, die auf seiner Plattform gespeichert werden, zu kontrollieren oder überwachen. Allerdings treffen ihn ab dem Zeitpunkt der Kenntnis im Rahmen der Störerhaftung Prüfpflichten zur Verhinderung von weiteren gleichartigen Rechtsverletzungen, deren Verletzung eine Unterlassungsverpflichtung begründen kann.[359]

Es ist zu bezweifeln, dass dies im Einklang mit europäischen Vorgaben ist, da dem Host-Provider durch diese Verpflichtung eine zusätzliche Voraussetzung auferlegt wird, die dieser erfüllen muss, um die Privilegierung des § 10 TMG bzw. Art. 14 ECRL in Anspruch zu nehmen und damit einer Haftung zu entgehen. Zudem kann gem. Art. 14 Abs. 3 ECRL lediglich ein Gericht oder eine

[358] So auch OLG Hamburg, MMR 2016, 269, 271; OLG Köln, GRUR 2014, 1081, 1089; KG Berlin, ZUM 2013, 886, 889; Hacker, GRUR-Prax 2011, 391, 393; Köhler in Köhler/Bornkamm, § 8 UWG, Rn. 2.28; Lorenz, jurisPR-ITR 6/2012 Anm. 4; Ohly, ZUM 2015, 308, 312; Ohly, GRUR 2010, 776, 784.

[359] Zu den Prüfpflichten im Rahmen der Störerhaftung, dem Kriterium der Zumutbarkeit sowie der Vereinbarkeit mit europarechtlichen Vorgaben siehe S. 131.

Verwaltungsbehörde vom Host-Provider verlangen, eine Rechtsverletzung abzustellen oder zu verhindern.[360] Die Prüfpflicht des Host-Providers tritt nach Kenntnis einer Rechtsverletzung jedoch automatisch ein, ohne Beteiligung eines Gerichts oder einer Verwaltungsbehörde. Es kann daher keine Rede von einer Anordnung im Sinne des Art. 14 Abs. 3 ECRL sein. Eine solche Anordnung sollte vielmehr unabhängig von der Feststellung einer Verantwortlichkeit des Host-Providers ergehen können.

Auch wenn man davon ausginge, dass der BGH weiterhin an einer Unanwendbarkeit der Haftungsprivilegien auf Unterlassungsansprüche festhält, so ergibt sich ein weitgehender Gleichlauf zwischen den Voraussetzungen des § 10 TMG und der deutschen Störerhaftung.[361] Daher wird teilweise auch die Meinung vertreten, dass der BGH zwar weiterhin an einer Unanwendbarkeit auf Unterlassungsansprüche festhielte, allerdings die Vorgaben des TMG und der ECRL in die Bewertung integriere.[362]

Nach § 10 S. 1 Nr. 1 TMG ist der Host-Provider privilegiert solange er keine Kenntnis von der Rechtsverletzung hat. Erlangt er Kenntnis von der Rechtsverletzung muss er gem. § 10 S. 1 Nr. 2 TMG unverzüglich tätig werden, wenn er seine Privilegierung nicht verlieren möchte.

Auch im Rahmen der Störerhaftung haftet der Host-Provider nicht solange er keine Kenntnis von der Rechtsverletzung hat. Nachdem er Kenntnis erlangt hat, muss er zunächst die entsprechende Rechtsverletzung beseitigen. Im Gegensatz zu § 10 TMG, welcher den Host-Provider weiterhin privilegiert, sofern er die Rechtsverletzung beseitigt, treffen ihn im Rahmen der Störerhaftung ab diesem Zeitpunkt allerdings Prüfpflichten, welchen er nachkommen muss, sofern er eine Unterlassungsverpflichtung nach nochmaliger Verletzung vermeiden möchte.

---

[360] Bezüglich der Möglichkeit von gerichtlichen Anordnungen gegen den Host-Provider siehe S. 134.

[361] Sieber/Höfinger in Hoeren/Sieber/Holznagel, Teil 18.1, Rn. 52; Lorenz, jurisPR-ITR 6/2012 Anm. 4.

[362] So bspw. AG Hamburg, BeckRS 2014, 13884.

hh) Fazit

Das Haftungsregime der Host-Provider hinsichtlich Urheberrechtsverletzungen ihrer Nutzer ist nach wie vor undurchsichtig. Durch seine Rechtsprechung hat der BGH nicht nur ein Haftungskonstrukt geschaffen, dass teilweise parallel zu dem nach europarechtlichen Vorgaben geschaffenem § 10 TMG läuft, sondern auch durch die unklare Verpflichtung zur Verhinderung weiterer kerngleicher Rechtsverletzungen im Rahmen der Störerhaftung eine Hürde geschaffen, welche der Host-Provider überwinden muss, um einer Haftung zu entgehen. Für die Rechteinhaber hingegen, ist diese Entwicklung vorteilhaft, da die Pflicht zur Aufdeckung und Beseitigung von Rechtsverletzung auf den Host-Provider verlagert wird.

c) Cache-Provider

Der Cache-Provider ist gemäß § 9 TMG, welcher Art. 13 ECRL umsetzt, für eine automatische, zeitlich begrenzte Zwischenspeicherung, welche allein dem Zweck dient, die Übermittlung fremder Informationen an andere Nutzer auf deren Anfrage effizienter zu gestalten, nicht verantwortlich, sofern er (1) die Informationen nicht verändert, (2) die Bedingungen für den Zugang zu den Informationen beachtet, (3) die Regeln für die Aktualisierung der Informationen, die in weithin anerkannten Industriestandards festgelegt sind, beachtet, (4) die erlaubte Anwendung von Technologien zur Sammlung von Daten über die Nutzung der Informationen, die in weithin anerkannten und verwendeten Industriestandards festgelegt sind, nicht beeinträchtigt und (5) unverzüglich handelt, um die gespeicherten Informationen zu entfernen oder den Zugang zu ihnen zu sperren, sobald sie Kenntnis davon erlangt haben, dass die Informationen am ursprünglichen Ausgangsort der Übertragung aus dem Netz entfernt wurden oder der Zugang zu ihnen gesperrt wurde oder ein Gericht oder eine Verwaltungsbehörde die Entfernung oder Sperrung angeordnet hat.

Die Haftungsprivilegierung des Cache-Providers wird folglich an die Erfüllung von fünf Voraussetzungen geknüpft.

aa) Anwendungsbereich

Damit der Anwendungsbereich des § 9 TMG überhaupt erst eröffnet ist, muss es sich um eine automatische, zeitliche begrenzte Zwischenspeicherung zum alleinigen Zweck der effizienteren Übermittlung von Informationen handeln. Bzgl. der maximalen Dauer der Speicherung gibt es keine gesetzlichen Vorgaben. In Abgrenzung zur kurzzeitigen Zwischenspeicherung i.S.d. § 8 Abs. 2 TMG erfasst § 9 TMG nicht lediglich die kurzzeitige Speicherung.[363]

Die Speicherungsdauer wird letzten Endes durch den Zweck der effizienten Übermittlung sowie der jeweiligen Art der konkreten Information bestimmt werden müssen und abhängig sein von dem Speichervolumen des spezifischen Servers.[364]

Eine automatische Zwischenspeicherung liegt vor, sofern der Cache-Provider keine eigene Entscheidung trifft.[365] Die Speicherung wird in diesem Fall vielmehr ohne weitere Willensbetätigung des Cache-Providers durch ein Programm gesteuert.[366]

Die Zwischenspeicherung darf zudem nur dem Zweck einer effizienteren Übermittlung fremder Informationen dienen. Effizienter ist die Übermittlung, worauf bereits die Überschrift des § 9 TMG hindeutet, wenn diese beschleunigt ist.[367] Dies ist beim sog. „Caching“ durch die Zwischenspeicherung von Informationen auf dem Proxy-Cache-Server regelmäßig der Fall. Auch wenn dies nicht ausdrücklich aus dem Wortlaut der Vorschrift ersichtlich ist, so hat die Zwischenspeicherung zu geschehen, weil die Information

[363] Hoffmann in Spindler/Schuster, § 9 TGM, Rn. 12. Nähere Ausführungen zur kurzzeitigen Zwischenspeicherung gem. § 8 Abs. 2 TMG siehe S. 93.
[364] Altenhain in MüKo zum StGB, § 9 TMG, Rn. 11; Hoffmann in Spindler/Schuster, § 9 TMG, Rn. 12.
[365] BT-Drucksache 14/6098, S. 24.
[366] Ott in BeckOK InfoMedienR, § 9 TMG, Rn. 11.
[367] Die Überschrift des Art. 13 ECRL hingegen spricht nicht von einer beschleunigten Übermittlung von Informationen, sondern lediglich von „Caching“.

zuvor bereits einmal durch einen anderen Nutzer abgerufen wurde.[368] Dies ergibt sich auch daraus, dass von einer Übermittlung an *andere* Nutzer die Rede ist.

Als Beispiel aus der Praxis können hierunter Usenet-Provider subsumiert werden, die Zugang zu Dateien im Usenet vermitteln und in dieser Funktion, durch Nutzeranfragen initiiert, Dateien im Usenet übermitteln und zwischenspeichern.

In der Rechtsprechung und im Schrifttum ist die Einordnung des Usenet-Providers allerdings umstritten. Korrekterweise ist bei der Einordnung des Usenet-Providers jeweils auf seine konkrete Tätigkeit im spezifischen Fall abzustellen.

Zunächst ist eine Einordnung des Usenet-Providers, der einen Newsserver betreibt und damit seinen eigenen Kunden auch die Möglichkeit eröffnet, Inhalte auf seinem eigenen Newsserver zu speichern, als Host-Provider möglich.[369] Handelt es sich bei den beanstandeten Inhalten also um solche, die auf dem Newsserver des Usenet-Providers gespeichert sind, ist er für diese nach den Bestimmungen des § 10 TMG privilegiert.

In Fällen, in denen der Usenet-Provider allerdings seinen Nutzern fremde Informationen übermittelt und lediglich zu diesem Zweck eine zeitlich begrenzte Zwischenspeicherung vornimmt, ist eine Einordnung als Cache-Provider geboten.[370] Denn hier werden die diversen Inhalte der Newsgroups zeitlich begrenzt auf seinem Servern zwischengespeichert, um bei einem erneuten Abruf eines Nutzers auf diese schneller zugreifen zu können, also letzten Endes zur Effizienzsteigerung.[371]

So urteilten auch das LG München I[372] und das OLG Düsseldorf[373], dass derjenige der einen kommerziellen Newsserver betreibt, über den er seinen Nutzern den Zugang zu diversen Newsgroups ermöglicht, für seine Tätigkeit nur als Cache-Provider haftet,

[368] So auch Altenhain in MüKo zum StGB, § 9 TMG, Rn. 7.
[369] So auch OLG Hamburg, MMR 2009, 631, 637.
[370] So auch Sieber/Höfinger in Hoeren/Sieber/Holznagel, Teil 18.1, Rn. 73.
[371] Sieber/Höfinger in Hoeren/Sieber/Holznagel, Teil 18.1, Rn. 73.
[372] LG München I, MMR 2007, 453, 454.
[373] OLG Düsseldorf, MMR 2008, 254, 255.

sofern der rechtsverletzende Inhalt auf einem anderen Newsserver gespeichert ist. In diesem Fall erfolgt eine zeitlich begrenzte Zwischenspeicherung dieser Inhalte auf dem eigenen Newsserver, die alleine dazu dient, die Übermittlung der fremden Information an andere Nutzer auf Anfrage effizienter zu gestalten.[374]

Abzulehnen ist die Ansicht des OLG Hamburg, welches den Usenet-Provider, der zwar selbst keinen Server betreibt, aber seinen Nutzern einen Newsreader zur Verfügung stellt, als Access-Provider im Sinne des § 8 TMG einordnete, da dieser lediglich den Zugang zu Dateien vermittle, die von anderen in das Usenet eingestellt wurden.[375] Das Gericht führt aus, dass zwar der Umstand, dass der Usenet-Provider eine einmalig abgerufene Nachricht zum beschleunigten Zugriff für 32 Stunden speichert dem Leitbild des § 9 TMG entspreche, dass dies aber keine weitergehende Verantwortlichkeit begründe, da die Möglichkeiten des Cache-Providers, eine Rechtsverletzung abzustellen, noch geringer seien als die eines Access-Providers.[376]

Die rechtliche Einordnung eines bestimmten Providers hat sich allerdings ausschließlich an der spezifischen Tätigkeit des Providers zu bemessen.

Abzulehnen sind zudem die Stimmen in der Literatur, die eine Einordnung als Cache-Provider ablehnen, da nicht die Beschleunigung der Übertragung im Vordergrund stehe, sondern es sich vielmehr eine selbstständige Zugriffsmöglichkeit handele, so dass hier generell § 10 TMG anwendbar sei.[377]

bb) Keine Veränderung der Information

Als erste der fünf Voraussetzungen, welche kumulativ vorliegen müssen, darf der Cache-Provider die Information nicht verändern. Hiervon nicht erfasst sind Eingriffe technischer Art im Laufe der Übermittlung, sofern diese die Integrität der Information nicht

[374] LG München I, MMR 2007, 453, 454; OLG Düsseldorf, MMR 2008, 254, 255.
[375] OLG Hamburg, MMR 2009, 405, 407; OLG Hamburg, MMR 2009, 631, 633.
[376] OLG Hamburg, MMR 2009, 631, 633.
[377] Altenhain in MüKo StGB, § 9 TMG, Rn. 8; Ott in BeckOK InfoMedienR, § 9 TMG, Rn. 8.

betreffen.[378] Hintergrund dieser Bestimmung ist, dass die dezentrale Kopie in jedem Moment dem Original entsprechen muss.[379]

cc) Beachten von Zugangsbedingungen

Der Cache-Provider muss zudem die Bedingungen für den Zugang zu den Informationen beachten. Laut Gesetzesbegründung soll dadurch vermieden werden, dass Zugangskontrollen einer Webseite unterlaufen werden.[380] Solche Zugangskontrollen können beispielsweise für die Gewährleistung des Jugendschutzes oder zur Sicherstellung der Bezahlung eines Entgelts eingerichtet worden sein und dürfen von dem Cache-Provider nicht umgangen werden.[381] Für die in der Praxis wohl am häufigsten vorkommende Zugangssperre, die Passwortabfrage, bedeutet dies, dass das Passwort zunächst auf dem Quellserver überprüft werden muss und erst dann die Information aus dem Zwischenspeicher des Proxy-Cache-Servers dargestellt werden darf.[382]

dd) Beachtung von Industriestandards für die Aktualisierung

Dritte Voraussetzung für die Privilegierung des Cache-Providers ist, dass dieser die Regeln für die Aktualisierung von Informationen, die in weithin anerkannten und verwendeten Industriestandards festgelegt sind, beachtet. Nach der Gesetzesbegründung sollen hiervon Fälle erfasst werden, in denen Informationen aktualisiert werden müssen und die Ursprungs-Webseite hierzu Angaben enthält.[383] Dadurch soll vermieden werden, dass eine bereits überholte Cache-Kopie den Eindruck vermittelt, sie entspreche der mittlerweile aktualisierten Ursprungs-Webseite.[384] Bedeutsam ist diese Bestimmung vor allem für

[378] BT-Drucksache 15/6098, S. 25.
[379] BT-Drucksache 15/6098, S. 25.
[380] BT-Drucksache 14/6098, S. 25.
[381] BT-Drucksache 14/6098, S. 25.
[382] Altenhain in MüKo zum StGB, § 9 TMG, Rn. 14; Hoffmann in Spindler/Schuster, § 9 TMG, Rn. 21.
[383] BT-Drucksache 14/6098, S. 25.
[384] BT-Drucksache 14/6098, S. 25.

Informationen auf Webseiten welche kontinuierlich aktualisiert werden, wie bspw. Börsen-Nachrichten.[385]

Vollkommen unklar ist allerdings worauf sich die weithin anerkannten und verwendeten Industriestandards beziehen. Weder die Begründung des TMG noch der ECRL führen hierzu weiter aus. Im Schrifttum wird darauf hingewiesen, dass entsprechende Industriestandards überhaupt nicht existieren.[386] *Altenhain* vertritt daher die Meinung, dass hier nicht Bezug genommen wird auf festgelegte Standards, wie bspw. DIN-Normen, da es solche ohnehin nicht gäbe, sondern vielmehr technikoffen die nach dem jeweiligen Stand von Wissenschaft und Technik entwickelten Standards gemeint seien.[387] Verlangt werde daher das aktuell technisch mögliche, in der Fachwelt anerkannte und in der Praxis bewährte Vorgehen, um eine Übermittlung aktueller Informationen zu gewährleisten.[388] Hieraus folgt, dass eine Aktualisierung spätestens beim Nutzer-Abruf erforderlich ist, indem der Cache-Provider zunächst bei der Ursprungs-Webseite nachfragt, ob eine neue bzw. aktualisierte Information vorliegt.[389]

ee) Keine Beeinträchtigung der Sammlung von Daten

Der Cache-Provider darf die erlaubte Anwendung von Technologien zur Sammlung von Daten über die Nutzung der Informationen, die in weithin anerkannten und verwendeten Industriestandards festgelegt sind, nicht beeinträchtigen. Nach der Gesetzesbegründung soll hierdurch vermieden werden, dass die Erfassung von Zugriffs-Zahlen durch Cache-Kopien unterlaufen wird.[390] Dies erlangt beispielsweise Bedeutung in Fällen, in denen sich die Höhe der Werbeeinnahmen nach der Häufigkeit der

[385] Ott in BeckOK InfoMedienR, § 9 TMG, Rn. 18.
[386] Hoffmann in Spindler/Schuster, § 9 TMG, Rn. 23.
[387] Altenhain in MüKo zum StGB, § 9 TMG, Rn. 15.
[388] Altenhain in MüKo zum StGB, § 9 TMG, Rn. 15; so im Ergebnis auch Hoffmann in Spindler/Schuster, § 9 TMG, Rn. 24.
[389] Altenhain in MüKo zum StGB, § 9 TMG, Rn. 15; Hoffmann in Spindler/Schuster, § 9 TMG, Rn. 28; Ott in BeckOK InfoMedienR, § 9 TMG, Rn. 19.
[390] BT-Drucksache 14/6098, S. 25.

Webseiten-Besuche richtet.[391] Würde in einem solchen Fall durch Cache-Kopien das installierte Zählsystem unterlaufen werden, so würde dem Inhaber der Ursprungs-Webseite hierdurch ein Schaden entstehen.[392] Ein weiteres Beispiel für eine solche Technologie zur Sammlung von Daten sind Cookies.[393] Zu beachten ist allerdings, dass die Datensammlung nur nicht beeinträchtigt werden darf, sofern diese erlaubt, das heißt auch rechtlich zulässig, ist und nicht bspw. unter Verletzung des Fernmeldegeheimnisses oder Datenschutzrechts erfolgt.[394] Eine dahingehende Prüfpflicht des Cache-Providers ist allerdings zu verneinen.[395]

Die Bestimmung verweist zudem auf anerkannte und verwendete Industriestandards hinsichtlich der Technologien zur Datensammlung, die der Inhaber der Ursprungs-Webseite zu beachten hat. Handelt es sich nicht um weithin anerkannte und verwendete Industriestandards, so trifft den Cache-Provider auch keine Verantwortlichkeit für den Fall, dass er diese beeinträchtigen sollte.[396]

Zur Umsetzung dieser Bestimmung muss der Cache-Provider seinen Dienst so einrichten, dass er anerkannte Methoden der Datensammlung unterstützt, so dass auch Zugriffe erfasst werden, bei denen die zwischengespeicherte Information übermittelt wird.[397]

ff) Unverzügliche Entfernung/Sperrung

Zu guter Letzt muss der Cache-Provider die Information entfernen oder den Zugang zu ihr zu sperren, sobald er Kenntnis davon erhalten hat, dass die Information auf der Ursprungs-Webseite aus dem Netz entfernt wurde oder der Zugang zu ihr gesperrt wurde oder ein Gericht oder eine Verwaltungsbehörde die Entfernung

[391] BT-Drucksache 14/6098, S. 25.
[392] BT-Drucksache 14/6098, S. 25.
[393] Altenhain in MüKo, § 9 TMG, Rn. 16; Hoffmann in Spindler/Schuster, § 9 TMG, Rn. 29; Sieber/Höfinger in Hoeren/Sieber/Holznagel, Teil 18.1, Rn. 76.
[394] Altenhain in MüKo zum StGB, § 9 TMG, Rn. 16; Hoffmann in Spindler/Schuster, § 8 TMG, Rn. 30.
[395] Hoffmann in Spindler/Schuster, § 9 TMG, Rn. 30; Ott in BeckOK InfoMedienR, § 9 TMG, Rn. 20.
[396] Hoffmann in Spindler/Schuster, § 9 TMG, Rn. 32.
[397] Altenhain in MüKo zum StGB, § 9 TMG, Rn. 16.

oder Sperrung angeordnet hat. Durch diese Bestimmung soll sichergestellt werden, dass die Inhalte, sofern diese auf der Ursprungs-Webseite nicht mehr enthalten sind, auch durch den Cache-Provider nicht mehr angezeigt werden.

Kenntnis im Sinne dieser Bestimmung ist die positive Kenntnis.[398] Während bereits durch § 9 S. 1 Nr. 3 TMG sichergestellt ist, dass dem Nutzer bei Nutzerabruf nicht mehr die gelöschte bzw. gesperrte Information übermittelt wird, so geht diese Bestimmung noch einen Schritt weiter und stellt die entsprechende Löschung bzw. Sperrung dieser Information unabhängig von einer bereits erfolgten Nutzeranfrage sicher.[399]

Die Löschung bzw. Sperrung seitens des Cache-Providers hat nach Wortlaut des TMG unverzüglich zu geschehen. Das europäische Pendant des Art. 13 ECRL hingegen spricht in der deutschen Fassung allerdings von einem zügigen Handeln des Cache-Providers. Die englische Fassung enthält keine entsprechende Unterscheidung und verwendet sowohl bei der Bestimmung betreffend den Host-Provider als auch bei der des Cache-Providers den Begriff *expeditiously*. Mangels unionsrechtlicher Definition dieses Begriffs ist auch hier auf den § 121 Abs. 1 S. 1 BGB zu rekurrieren und auf ein Handeln ohne schuldhaftes Zögern zurückzugreifen.[400]

Nach der Gesetzesbegründung kann zudem auch vom Cache-Provider nur das verlangt werden, was technisch möglich und zumutbar ist.[401]

gg) Keine Zusammenarbeit mit dem Nutzer

§ 9 S. 2 TMG nimmt Bezug auf § 8 Abs. 1 S. 2 TMG und erklärt diesen für den Cache-Provider entsprechend anwendbar. Damit entfällt die Privilegierung im Falle einer absichtlichen

---

[398] Altenhain in MüKo zum StGB, § 9 TMG, Rn. 18; Ott in BeckOK InfoMedienR, § 9 TMG, Rn. 22.

[399] Altenhain in MüKo zum StGB, § 9 TMG, Rn. 18; Ott in BeckOK TMG, § 9 Rn. 22.

[400] So auch Altenhain in MüKo zum StGB, § 9 TMG, Rn. 19; a.A. Sieber/Höfinger in Hoeren/Sieber/Holznagel, Teil 18.1, Rn. 77.

[401] BT-Drucksache 14/6098, S. 25.

Zusammenarbeit zwischen Cache-Provider und Nutzer, sofern diese geschieht um rechtswidrige Handlungen zu begehen.

hh) Anwendbarkeit auf Unterlassungsansprüche

Sowohl im Schrifttum wie auch in der Rechtsprechung wird der Cache-Provider kaum behandelt. Die bisher zum Cache-Provider ergangene unterinstanzliche Rechtsprechung geht, jeweils mit Bezug auf die „Internetversteigerung I"-Rechtsprechung des BGH, prinzipiell davon aus, dass auch im Falle des Cache-Providers die Privilegien des TMG auf Unterlassungsansprüche keine Anwendung finden.

Ohne weitere Begründung führen sowohl das OLG Düsseldorf als auch das LG München I aus, dass nach der Rechtsprechung des BGH die Haftungsprivilegien des TMG nicht auf verschuldensunabhängige Unterlassungsansprüche anzuwenden seien.[402]

Die von den Gerichten angenommene Unanwendbarkeit des § 9 TMG auf Unterlassungsansprüche ist jedoch im Hinblick auf die europarechtlichen Vorgaben zweifelhaft. Hier kann auf die für den Host-Provider aufgeführten Gründe sowie die ergänzenden Ausführungen zum Access Provider zurückgegriffen werden.[403]

Zudem ist es insbesondere vor dem Hintergrund, dass § 9 S. 1 Nr. 5 TMG lediglich eine Entfernung bzw. Sperrung anordnet, sofern das Material am ursprünglichen Ausgangsort entfernt wurde, bedenklich eine Prüfpflicht im Rahmen der Störerhaftung auch für Materialien anzunehmen, die weiterhin noch auf dem Ursprungsserver vorhanden sind. Dies würde im klaren Widerspruch zu den Privilegierungsvoraussetzungen des § 9 TMG stehen.

[402] OLG Düsseldorf, MMR 2008, 254, 255; LG München I, MMR 2007, 453, 455.

[403] Siehe S. 65 hinsichtlich des Host-Providers sowie S. 108 hinsichtlich des Access-Providers.

ii) Fazit

Es ist davon auszugehen, dass der Cache-Provider auch in Zukunft in der Praxis keine nennenswerte Rolle spielen wird.

Im Bereich des Usenets ist dies auch darauf zurückzuführen, dass im Falle einer Rechtsverletzung eine primäre Inanspruchnahme des Host-Providers, d.h. des Providers des Newsservers auf dem der Inhalt ursprünglich gespeichert wurde, wesentlich effektiver ist und vor Inanspruchnahme des Cache-Providers ohnehin notwendig ist. Zudem wird die Information ohnehin nur zeitlich begrenzt vom Cache-Provider zwischengespeichert und der Cache-Provider ist dazu angehalten, überholte Cache-Kopien, soweit möglich, zu aktualisieren.

d) Access Provider

Der Access-Provider ist gem. § 8 TMG, welcher Art. 12 ECRL umsetzt, nicht für fremde Informationen, die er in einem Kommunikationsnetz übermittelt oder zu denen er den Zugang zur Nutzung vermittelt, verantwortlich, sofern er (1) die Übermittlung nicht veranlasst hat, (2) den Adressaten der übermittelten Information nicht ausgewählt und (3) die übermittelten Informationen nicht ausgewählt oder verändert hat.

Bereits § 5 Abs. 3 S. 1 TDG a.F. enthielt die Bestimmung, dass Access-Provider nicht für Inhalte verantwortlich sind, zu denen sie lediglich den Zugang zur Nutzung vermitteln. In Umsetzung des Art. 12 ECRL ist die Privilegierung nunmehr an mehrere Bedingungen geknüpft, welche der Access-Provider kumulativ erfüllen muss.

aa) Anwendungsbereich

Unter den Oberbegriff der Durchleitung fallen zwei unterschiedliche Vorgänge. Privilegiert ist sowohl die Übermittlung von fremden Informationen in einem

Kommunikationsnetzwerk[404] als auch die Vermittlung des Zugangs zu fremden Informationen.[405]

Die erste Alternative behandelt Fälle des sog. Routing, in denen der Diensteanbieter den Transport einer Information vom Absender zum Empfänger steuert und damit eine Übermittlungsdienstleistung erbringt.[406] Der Diensteanbieter agiert hier als sog. Network-Provider, der eine Telekommunikationsinfrastruktur bereithält und dem Nutzer die Nutzung seiner Übertragungskapazitäten anbietet.[407] Hierunter fällt bspw. das Weiterleiten der Kopie einer abgerufenen Webseite oder von E-Mails eines Anbieters von E-Mail-Diensten.[408]

Die zweite Alternative betrifft die Tätigkeit des Access-Providers, welche darin besteht, dem Nutzer Zugang zu einem Computernetzwerk, insbesondere dem Internet, zu verschaffen und damit die Nutzung fremder Informationen überhaupt erst ermöglichen.[409] Hierunter fallen demnach grundsätzlich auch Betreiber eines WLAN.[410]

Im Folgenden werden beide Tätigkeiten unter dem Begriff des Access-Providers gefasst. Auch in der Praxis werden die Tätigkeiten dieser Provider oftmals zusammenfallen.

bb) Keine Veranlassung der Übermittlung

Erste Voraussetzung gem. § 8 Abs. 1 S. 1 Nr. 1 TMG für eine Privilegierung des Access-Providers ist, dass dieser die Übermittlung nicht veranlasst hat. Er darf folglich weder der Initiator einer solchen Übermittlung sein noch in irgendeiner Weise auf den Nutzer hinsichtlich der Übermittlung Einfluss nehmen.[411]

---

[404] § 8 Abs. 1 S. 1 Alt. 1 TMG.
[405] § 8 Abs. 1 S. 1 Alt. 2 TMG.
[406] Hoffmann in Spindler/Schuster, § 8 TMG, Rn. 16; Paal in BeckOK InfoMedienR, § 8 TMG, Rn. 14.
[407] Altenhain in MüKo zum StGB, § 1 TMG, Rn. 15.
[408] Altenhain in MüKo zum StGB, Vorbemerkung zu den §§ 7 ff. TMG, Rn. 52.
[409] Altenhain in MüKo zum StGB, Vorbemerkung zu den §§ 7 ff. TMG, Rn. 48.
[410] Altenhain in MüKo zum StGB, Vorbemerkung zu den §§ 7 ff. TMG, Rn. 48; Sieber/Höfinger in Hoeren/Sieber/Holznagel, Teil 18.1, Rn. 64. Hinsichtlich der Problematik und Diskussion zur Anwendbarkeit der Privilegien auf private und öffentliche WLAN-Betreiber siehe S. 95.
[411] Altenhain in MüKo zum StGB, § 8 TMG, Rn. 7.

cc) Keine Auswahl des Adressaten

Weiterhin darf der Access-Provider gem. § 8 Abs. 1 S. 1 Nr. 2 TMG den Adressaten der Informationen nicht ausgewählt haben. Die Auswahl muss ausschließlich vom Nutzer ausgehen.[412] Nicht gedeckt sind somit jegliche Arten von Filterfunktionen, welche sich dahingehend äußern, dass dadurch einzelne Empfänger auserwählt oder geblockt werden.[413]

dd) Keine Auswahl oder Veränderung der übermittelten Informationen

Als dritte und letzte Voraussetzung darf der Access-Provider gem. § 8 Abs. 1 S. 1 Nr. 3 TMG die übermittelten Informationen nicht ausgewählt oder verändert haben. Auch hier muss folglich die Initiative darüber, welche Informationen übermittelt werden sollen, vom Nutzer ausgehen. Nicht erfasst von dem Begriff des Veränderns sind solche Veränderungen, die lediglich technischer Natur sind und die nicht die Integrität der Information betreffen.[414] Hierunter fällt bspw. die für die Übermittlung notwendige Zerlegung der Information in Datenpakete und die Datenkompression zur schnelleren Übermittlung.[415]

ee) Keine Zusammenarbeit mit dem Nutzer

Eine Privilegierung des Access-Providers entfällt gem. § 8 Abs. 1 S. 2 TMG auch, sofern dieser absichtlich mit dem Nutzer seines Dienstes zusammengearbeitet hat, um rechtswidrige Handlungen zu begehen.

Dieser Zusatz hat kein entsprechendes Pendant in Art. 12 ECRL, allerdings findet sich fast wortgleich derselbe Gedanke in Erwägungsgrund 44 wieder. Im deutschen Recht geht er auf einen Klarstellungswunsch des Bundesrates zurück.[416] Allerdings dürften in einem solchen Fall der absichtlichen Zusammenarbeit zur Begehung rechtswidriger Handlungen bereits die zuvor genannten

[412] Altenhain in MüKo zum StGB, § 8 TMG, Rn. 8.
[413] Hoffmann in Spindler/Schuster, § 8 TMG, Rn. 22.
[414] BT-Drucksache 14/6098, S. 24.
[415] Altenhain in MüKo zum StGB, § 8 TMG, Rn. 9.
[416] BT-Drucksache 14/6098, S. 33.

Haftungsausschlusskriterien des § 8 Abs. 1 S. 1 Nr. 1-3 TMG schon nicht erfüllt sein.[417] Dieser Bestimmung kommt somit hauptsächlich eine klarstellende Funktion zu, sie hat weder eine eigenständige praktische noch theoretische Bedeutung.[418]

Erforderlich für die Erfüllung der absichtlichen Zusammenarbeit ist nach h.M. jedenfalls ein zielgerichtetes Wollen in Form des Vorsatzes seitens des Access-Providers.[419] Der Begriff der Zusammenarbeit ist sowohl im Sinne einer Mittäterschaft als auch einer Beihilfe oder Anstiftung zu verstehen.[420]

ff) Gleichstellung automatischer kurzzeitiger Zwischenspeicherung

Der Übermittlung der Information und der Zugangsvermittlung zu dieser wird gem. § 8 Abs. 2 TMG auch deren automatische kurzzeitige Zwischenspeicherung gleichgesetzt, sofern diese nur zur Durchführung der Übermittlung geschieht und die Speicherung nicht länger erfolgt, als für die Übermittlung üblicherweise erforderlich ist. Im Gegensatz zu § 9 TMG, welcher eine zeitlich begrenzte Zwischenspeicherung privilegiert, bezieht sich die kurzzeitige Zwischenspeicherung des Access-Providers nicht auf Zwecke zur effizienteren Datenübermittlung, sondern ist technisch zur Ermöglichung einer Nutzeranfrage erforderlich.[421]

Die kurzzeitige Speicherung gilt demnach als Bestandteil des Übermittlungs- bzw. Zugangsvermittlungsvorgangs sofern die folgenden Voraussetzungen erfüllt sind.

---

[417] Hoffmann in Spindler/Schuster, § 8 TMG, Rn. 32; Paal in BeckOK InfoMedienR, § 8 TMG, Rn. 26.

[418] Hoffmann in Spindler/Schuster, § 8 TMG, Rn. 32; Paal in BeckOK InfoMedienR, § 8 TMG, Rn. 26.

[419] Altenhain in MüKo zum StGB, § 8 TMG, Rn. 11; Hoffmann in Spindler/Schuster, § 8 TMG, Rn. 31; Paal in BeckOK InfoMedienR, § 8 TMG, Rn. 27; Sieber/Höfinger in Spindler/Schuster, Teil 18.1, Rn 69; Vassilaki, MMR 2002, 659, 660.

[420] Altenhain in MüKo zum StGB, § 8 TMG, Rn. 11; Hoffmann in Spindler/Schuster, § 8 TMG, Rn. 31; Paal in BeckOK InfoMedienR, § 8 TMG, Rn. 29.

[421] Ott in BeckOK InfoMedienR, § 9 TMG, Rn. 1.

(1) Automatische kurzzeitige Zwischenspeicherung

In Abgrenzung zum Host-Provider i.S.d. § 10 TMG, der Informationen auf Dauer speichert und zu dem Cache-Provider i.S.d. § 9 TMG, der Informationen für eine gewisse Dauer speichert, ist von § 8 Abs. 2 TMG nur die kurzzeitige Ablage einer Information erfasst. Das Kriterium der Kurzzeitigkeit wird dadurch bestimmt, dass die Information nicht länger gespeichert werden darf, als dies für die Übermittlung üblicherweise erforderlich ist.[422] Zudem muss die Zwischenspeicherung aus einem automatischen Vorgang folgen, d.h. es kommt nicht auf einen Willensakt des Access-Providers an.[423]

(2) Nur zur Durchführung der Übermittlung

Die automatische und kurzzeitige Speicherung darf nur für die Durchführung der Übermittlung geschehen. Sie hat aus rein technischen Gründen zu erfolgen.[424] Hierunter fällt bspw. die beim Routing von Informationen größeren Datenvolumens aus Gründen der Netzkapazität notwendige Aufteilung und Zwischenspeicherung kleiner Datenpakete während des Übertragungsvorgangs.[425]

Durch den Zusatz „nur“ wird nochmals klargestellt, dass die Zwischenspeicherung lediglich für die Durchführung der Übermittlung erfolgen darf. Sofern sie auch für andere Zwecke, wie bspw. die beschleunigte Übermittlungen von Informationen erfolgt, wäre in diesem Fall nicht mehr § 8 TMG, sondern § 9 TMG einschlägig.[426]

(3) Keine längere Speicherung als üblicherweise erforderlich

Die Zwischenspeicherung darf zudem nicht länger als üblicherweise erforderlich erfolgen. Durch die Beschränkung der

---

[422] Altenhain in MüKo zum StGB, § 8 TMG, Rn. 15; Hoffmann in Spindler/Schuster, § 8 TMG, Rn. 39.
[423] Hoffmann in Spindler/Schuster, § 8 TMG, Rn. 38; Paal in BeckOK TMG, § 8 Rn. 33.
[424] Paal in BeckOK InfoMedienR, § 8 TMG, Rn. 35.
[425] Hoffmann in Spindler/Schuster, § 8 TMG, Rn. 40; Paal in BeckOK InfoMedienR, § 8 TMG, Rn. 35.
[426] Hoffmann in Spindler/Schuster, § 8 TMG, Rn. 40.

Erforderlichkeit auf das Übliche, welche auf Art. 12 Abs. 2 ECRL basiert, sind theoretisch auch Vorgänge, welche länger als erforderlich andauern, allerdings im Bereich des Üblichen liegen, privilegiert.[427]

gg) Anwendbarkeit auf WLAN-Betreiber

Am 27. Juli 2016 ist das Zweite Gesetz zur Änderung des TMG in Kraft getreten („WLAN Gesetz"). Hierdurch wurde § 8 TMG um einen Absatz 3 erweitert, welcher klarstellt, dass § 8 Abs. 1 und Abs. 2 auch für Diensteanbieter gelten, die Nutzern einen Internetzugang über ein drahtloses lokales Netzwerk zur Verfügung stellen.

Bereits vor Einführung des WLAN-Gesetzes, ging die h.M. im Schrifttum davon aus, dass grundsätzlich auch WLAN-Betreiber unter den Anwendungsbereich des § 8 TMG.[428]

Aufgrund der Definition des Diensteanbieters in § 2 S. 1 Nr. 1 TMG als jede natürliche oder juristische Person, die den Zugang zur Nutzung vermittelt, war die h.M. der Auffassung, dass hiervon sowohl private als auch gewerbliche WLAN-Anbieter umfasst sind.[429] Dies folgte bereits aus der Gesetzesbegründung, wo explizit ausgeführt wird, dass es für das Eingreifen der Privilegien nach §§ 8-10 TMG unerheblich ist, ob die Informationen geschäftsmäßig oder nur privat übermittelt oder gespeichert werden.[430]

Es ist jedoch strittig, ob der Begriff des Diensteanbieters i.S.d. TMG über die Definition des Dienstes der Informationsgesellschaft auf europäischer Ebene hinausgeht.[431] Denn gem. Art. 2 lit. a) ECRL sind Dienste der Informationsgesellschaft Dienste i.S.d. Art. 1 Nr. 2 der RL 98/34/EG in der Fassung der RL 98/48/EG, welcher

[427] Altenhain in MüKo zum StGB, § 8 TMG, Rn. 15.
[428] Altenhain in MüKo zum StGB, § 8 TMG, Rn. 3; Hoffmann in Spindler/Schuster, § 8 TMG, Rn. 17; Sieber/Höfinger in Hoeren/Sieber/Holznagel, Teil 18.1, Rn. 64; Hoeren/Jakopp, ZRP 2014, 72, 73; Mantz, GRUR-RR 2013, 497, 498.
[429] Altenhain in MüKo zum StGB, § 1 TMG, Rn. 8; Sieber/Höfinger in Hoeren/Sieber/Holznagel, Teil 18.1, Rn. 64; Hoeren/Jakopp, ZRP 2014, 72, 75; Mantz, MMR 2006, 763, 765; Stang/Hühner, GRUR-RR 2008, 273, 275.
[430] BT-Drucksache 14/6098, S. 23.
[431] So z.B. Sieber/Höfinger in Hoeren/Sieber/Holznagel, Teil 18.1, Rn. 30.

besagt, dass dies jede in der Regel gegen Entgelt elektronisch im Fernabsatz und auf individuellen Abruf eines Empfängers erbrachte Dienstleitung ist. Teilweise wird daher argumentiert, dass lediglich kommerzielle Anbieter nach der europäischen Definition erfasst seien.[432]

§ 8 TMG fand in der Rechtsprechung in Bezug auf die Bereitstellung offener WLAN bislang jedenfalls wenig Beachtung.

(1) BGH Rechtsprechung zu privaten WLAN-Anschluss

Im Jahr 2010 erging die erste höchstinstanzliche Entscheidung zur Verantwortlichkeit privater WLAN-Inhaber für über diesen Anschluss begangene Urheberrechtsverletzungen. In der Entscheidung „Sommer unseres Lebens“[433] entschied der I. Zivilsenat, dass der Inhaber eines WLAN-Anschlusses dazu verpflichtet ist, diesen ausreichend gegen Zugriffe Dritter zu schützen.[434] Ihn treffe insofern eine Prüfungspflicht, deren Verletzung zu einer Haftung als Störer führe.[435] Die ihm zumutbaren Maßnahmen müssten allerdings im Rahmen des technisch Möglichen liegen.[436] Für den privaten Verwender der WLAN-Technologie bedeute dies, dass er die im Kaufzeitpunkt des WLAN-Routers marktüblichen Sicherungen anzuwenden habe.[437] Unterlasse er dies, so hafte er als Störer auf Unterlassung, wenn Dritte in der Folge diesen Anschluss nutzen, um Urheberrechtsverletzungen darüber zu begehen.[438]

Der BGH führt in diesem Zusammenhang aus, dass den WLAN-Anschlussinhaber diese Prüfpflichten nicht erst treffen, nachdem dieser von einer unbefugten Nutzung seines Anschlusses erfahren hat und es somit bereits zu seiner Rechtsverletzung durch einen

[432] Sieber/Höfinger in Hoeren/Sieber/Holznagel, Teil 18.1, Rn. 30.
[433] BGHZ 185, 330 = GRUR 2010, 633.
[434] BGH GRUR 2010, 633, 635.
[435] BGH GRUR 2010, 633, 635.
[436] BGH GRUR 2010, 633, 635.
[437] BGH GRUR 2010, 633, 635.
[438] BGH GRUR 2010, 633, 635.

Dritten gekommen ist, sondern bereits ab Inbetriebnahme des Anschlusses.[439]

Er nimmt hier Bezug auf die BGH-Urteile zur Internetversteigerung sowie auf den § 10 TMG bzw. Art. 14 ECRL, welche er in der Folge als nicht anwendbar erklärt.[440]

(2) Bewertung der Rechtsprechung zu privaten WLAN-Anschluss

Überraschend ist die Bezugnahme des BGH auf die „Internetversteigerungs"-Urteile sowie die hieran folgende Anknüpfung an § 10 TMG bzw. Art. 14 ECRL, welchen er anschließend richtigerweise als nicht einschlägig verwirft.

Insoweit ist dem BGH zwar zuzustimmen, da es sich bei dem WLAN-Anschlussinhaber nicht um einen Host-Provider i.S.d. TMG handelt, welcher Speicherkapazitäten für seine Nutzer zur Verfügung stellt, sondern um einen Access-Provider, welcher einem Dritten den Zugang zum Internet vermittelt. Deshalb ist auch eine Bezugnahme auf die Kenntnis des Anschlussinhabers zu Recht verneint worden, da diese bei der Frage der Privilegierung des Access-Providers bekanntermaßen keine Rolle spielt.

Fragwürdig ist allerdings der durch den Gerichthof hieraus gezogene Schluss, dass den Anschlussinhaber bereits ab Nutzung des WLAN eine Prüfpflicht als Störer trifft.[441] Der erkennende Senat hätte hier vielmehr die spezifischen Voraussetzungen für eine Privilegierung des Access-Providers prüfen müssen.

Er übersieht jedoch offensichtlich die, jedenfalls potentielle, Einschlägigkeit des § 8 TMG und geht mit keinem Wort auf eine entsprechend denkbare Haftungsprivilegierung des Anschlussinhabers aufgrund des TMG ein.[442]

---

[439] BGH GRUR 2010, 633, 635.
[440] BGH GRUR 2010. 633, 635.
[441] So auch Ernst, MMR 2007, 538, 539; Hoeren/Jakopp, ZRP 2014, 72, 74; Mantz/Gietl, MMR 2008, 606, 607.
[442] Hoeren/Jakopp, ZRP 2014, 72, 73; Stang/Hühner, GRUR 2010, 636, 637.

(3) Abweichende unterinstanzliche Rechtsprechung zu privatem WLAN-Anschluss

Entgegen der BGH-Entscheidung entschied das AG Berlin-Charlottenburg im Jahr 2014, dass der Inhaber eines privaten ungesicherten WLAN-Anschlusses, welchen er jedem beliebigen Dritten zur Verfügung stellt, nicht als Störer haftet.[443] Der Anschlussinhaber bot dabei seinen WLAN-Anschluss im Rahmen der sog. Freifunk-Initiative[444] unbekannten Dritten zur freien Nutzung an. Das Gericht wies hier zunächst auf die grundsätzliche Anwendbarkeit von § 8 TMG auf Personen, welche ein öffentliches WLAN anbieten, hin.[445] Diese Privilegierung greife zwar nicht für Unterlassungsansprüche, allerdings wären in solchen Fällen an die Zumutbarkeit von Maßnahmen im Rahmen der Störerhaftung besonders strenge Anforderungen zu stellen.[446] Dem WLAN-Betreiber dürfe nichts abverlangt werden, was sein Geschäftsmodell gefährde, wozu u.a. Port- oder DNS-Sperren, Registrierungs- und Belehrungspflichten gehörten.[447]

(4) Rechtsprechung zu gewerblichen WLAN-Anschlüssen

Hinsichtlich gewerblich betriebener WLAN-Anschlüsse gibt es bislang keine höchstrichterliche Rechtsprechung, allerdings haben sich einige untere Instanzgerichte mit der Haftungsfrage auseinandergesetzt und sind diesbezüglich zu unterschiedlichen Ergebnissen gelangt.

Auch hier wurde zunächst die Frage der Haftung völlig ungeachtet einer etwaigen Privilegierung durch § 8 TMG betrachtet. Das LG Frankfurt gelangte so zu dem Ergebnis, dass der Hotelbetreiber, welcher seinen Gästen die Nutzung seines WLAN zur Verfügung stellte, jedenfalls nicht als Störer hafte, sofern er den Zugang gegenüber anderweitigem Zugriff Dritter verschlüsselt habe und seine Gäste auf die Einhaltung gesetzlicher Vorschriften

[443] AG Berlin-Charlottenburg, GRURRS 2015, 02858.
[444] Siehe hierzu auch https://freifunk.net, zuletzt besucht am 23.04.2016.
[445] AG Berlin-Charlottenburg, GRUR-RS 2015, 02858.
[446] AG Berlin-Charlottenburg, GRUR-RS 2015, 02858.
[447] AG Berlin-Charlottenburg, GRUR-RS 2015, 02858.

hingewiesen habe.[448] Ähnlich entschied das gleiche Gericht in dem Fall eines Vermieters einer Ferienwohnung, welcher seinen Mietern den Zugang explizit nur zur beruflichen Nutzung sowie zum Versand von E-Mails eröffnet hatte.[449] Diese einschränkende Nutzungsüberlassung sah das Gericht als ausreichend an, um einer Haftung als Störer zu entgehen.[450]

Im Gegensatz hierzu steht die Rechtsprechung des LG Hamburg, in der es um die Haftung des Betreibers eines Internetcafés für Urheberrechtsverletzungen seiner Gäste ging.[451] In einer knappen Begründung führte das Gericht aus, dass dem Inhaber des Internetcafés als Störer Maßnahmen zumutbar und möglich seien, um Urheberrechtsverletzungen, in diesem Fall die Bereitstellung urheberrechtlich geschützter Dateien in Filesharing-Programmen, zu verhindern.[452] Insbesondere könne er die für ein Filesharing erforderlichen Ports sperren.[453] Da er dies nicht getan habe, hafte er folglich verschuldensunabhängig auf Unterlassung.[454]

Es ist allerdings auch hier in der neueren Rechtsprechung eine Kehrtwende zu erkennen. So ergingen im Jahr 2014 drei Urteile hinsichtlich der Haftung gewerblicher WLAN-Anbieter, in welchen die Gerichte jeweils die grundsätzliche Privilegierung des gewerblichen WLAN-Anbieters als Access-Provider und entsprechende Anwendbarkeit des § 8 TMG anerkannten.[455]

Das AG Hamburg ging allerdings noch von einer Unanwendbarkeit des § 8 TMG auf Unterlassungsansprüche und damit auf die Störerhaftung aus, lies die Inanspruchnahme des Vermieters einer Ferienwohnung bzw. des Hotelbetreibers letzten Endes aber daran scheitern, dass diese den WLAN-Anschluss ausreichend verschlüsselt sowie die Mieter über die rechtmäßige

[448] LG Frankfurt, MMR 2011, 401.
[449] LG Frankfurt, MMR 2013, 507.
[450] LG Frankfurt, MMR 2013, 507, 509.
[451] LG Hamburg, MMR 2011, 475.
[452] LG Hamburg, MMR 2011, 475, 475.
[453] LG Hamburg, MMR 2011, 475, 475.
[454] LG Hamburg, MMR 2011, 475, 475.
[455] AG Hamburg, BeckRS 2014, 13884; AG Hamburg, ZUM-RD 2015, 207; LG München I, ZUM 2015, 344. Dies gilt laut Auffassung der Gerichte sowohl für private als auch gewerbliche WLAN-Anbieter.

Internetnutzung ordnungsgemäß belehrt haben.[456] Allerdings merkte das Gericht hier bereits an, dass es fraglich sei, ob der private WLAN-Betreiber überhaupt zu einer solchen Belehrung verpflichtet sei, da er damit gegenüber dem „klassischen" Provider benachteiligt wäre, da diesen keine entsprechenden Belehrungspflichten träfen.[457]
Die Unanwendbarkeit des § 8 TMG auf Unterlassungsansprüche sah das LG München I aber gerade als fraglich an und hat in einem umfassenden Vorabentscheidungsersuchen dem EuGH insgesamt neun Fragen hinsichtlich der Auslegung der Vorschriften zur Verantwortlichkeit des Access-Providers vorgelegt.[458]

(5) Vorabentscheidungsersuchen des LG München I

In dem Fall der dem LG München I zur Beurteilung vorliegt, geht es um die Verantwortlichkeit eines gewerblichen WLAN-Betreibers im Rahmen der Störerhaftung. Das LG München I sah sich hier einer Reihe von Auslegungsfragen hinsichtlich der ECRL ausgesetzt und hat in der Folge dem EuGH die folgenden Fragen vorgelegt:

(a) Die erste Frage betrifft den Begriff des Dienstes der Informationsgesellschaft, mit der das Gericht klären will, ob der WLAN-Betreiber überhaupt einen solchen Dienst anbietet. Art. 2 lit. a) ECRL bezieht sich auf Bestimmung des Ausdrucks „Dienst der Informationsgesellschaft" auf den des „Dienstes" gem. Art. 1 Nr. 2 der Richtlinie 98/34/EG in der Fassung der Richtlinie 98/48/EG. Danach ist eine Dienstleistung der Informationsgesellschaft jede in der Regel gegen Entgelt elektronisch im Fernabsatz und auf individuellen Abruf eines Empfängers erbrachte Dienstleistung. Zur Beurteilung, ob hierunter auch der WLAN-Betreiber fällt, ersucht das LG München I die

[456] AG Hamburg, BeckRS 2014, 13884; AG Hamburg, ZUM-RD 2015, 207, 209.
[457] AG Hamburg, BeckRS 2014, 13884; AG Hamburg, ZUM-RD 2015, 207, 209.
[458] LG München I, ZUM 2015, 344, beim EuGH anhängig unter C-484/14 – „Mc Fadden".

Auslegung des Begriffs „in der Regel gegen Entgelt“. Es möchte wissen, ob dies bedeutet, dass (a) die konkret betroffene Person, die sich auf die Diensteanbietereigenschaft beruft, diese konkrete Dienstleistung in der Regel entgeltlich anbietet oder (b) überhaupt Anbieter auf dem Markt sind, die diese Dienstleistung oder vergleichbare Dienstleistungen gegen Entgelt anbieten oder (c) die Mehrheit dieser oder vergleichbarer Dienstleistungen gegen Entgelt angeboten werden.[459]

(b) Mit der zweiten Frage ersucht das Gericht die Auslegung des Begriffs „Zugang zu einem Kommunikationsnetzwerk zu vermitteln“ gem. Art. 12 Abs. 1 ECRL und möchte damit wissen, ob es hierfür lediglich darauf ankommt, dass der Erfolg der Zugangsvermittlung eintritt.[460]

(c) Die dritte Frage richtet sich auf die Auslegung des Begriffs „anbieten“ gem. Art. 2 lit. b) ECRL, da hiernach jede natürliche oder juristische Person als Diensteanbieter klassifiziert wird, die einen Dienst der Informationsgesellschaft anbietet. Das Gericht möchte wissen, ob es für ein „Anbieten“ in diesem Sinne ausreicht, wenn der Dienst rein tatsächlich zur Verfügung gestellt wird, im vorliegenden Fall also ein offenes WLAN bereitgestellt wird, oder ob darüber hinaus ein „Anpreisen“ erforderlich ist.[461]

(d) Die vierte Frage bezieht sich auf den Begriff „nicht für die übermittelten Informationen verantwortlich“ des Art. 12 Abs. 1 ECRL. Das Gericht möchte wissen, ob dies bedeutet, dass etwaige Ansprüche auf Unterlassung, Schadensersatz, Zahlung der Abmahnkosten und Gerichtsgebühren gegen den Access-Provider grundsätzlich oder jedenfalls in Bezug auf eine erste festgestellte Urheberrechtsverletzung ausgeschlossen sind.[462]

---

[459] LG München I, ZUM 2015, 344, 348.
[460] LG München I, ZUM 2015, 344, 349.
[461] LG München I, ZUM 2015, 344, 349.
[462] LG München I, ZUM 2015, 344, 349 f.

(e) Die fünfte Frage bezieht sich auf das Spannungsverhältnis von Art. 12 Abs. 1 ECRL und Art. 12 Abs. 3 ECRL. Das Gericht möchte geklärt wissen, ob dies dahingehend zu verstehen ist, dass gegen den Access-Provider keine Anordnung erlassen werden kann, wonach es dieser künftig zu unterlassen hat, Dritten zu ermöglichen, über einen konkreten Internetanschluss ein bestimmtes urheberrechtlich geschütztes Werk zum Abruf bereitzustellen.[463]

(f) Die sechste Frage betrifft die Auslegung des normativen Spannungsverhältnisses von Art. 12 Abs. 1 ECRL und Art. 14 Abs. 1 lit. b) ECRL und die Frage, ob der Access-Provider in entsprechender Anwendung von Art. 14 Abs. 1 lit. b) ECRL verantwortlich ist, sobald er Kenntnis von der konkreten Rechtsverletzung hat und nicht unverzüglich tätig wird, um künftige derartige Rechtsverletzungen über seinen Zugang durch verkehrsübliche Sicherungsmaßnahmen zu verhindern. Das Gericht möchte wissen, ob Art. 12 Abs. 1 ECRL dahingehend auszulegen ist, dass unter den Umständen des Ausgangsverfahrens Art. 14 Abs. 1 lit. b) ECRL entsprechend auf einen Unterlassungsanspruch anzuwenden ist.[464]

(g) Mit der siebten Frage möchte das Gericht wissen, ob Art. 12 Abs. 1 ECRL in Verbindung mit Art. 2 lit. b) ECRL dahingehend auszulegen ist, dass sich die Anforderungen an den Diensteanbieter darin erschöpfen, dass dies jede natürliche oder juristische Person ist, die einen Dienst der Informationsgesellschaft anbietet.[465]
Im Falle des WLAN-Betreibers wäre laut Gericht beispielsweise als zusätzliche Voraussetzung denkbar, dass zwischen dem eigentlichen Geschäftszweck des Gewerbetreibenden und dem Bereithalten des offenen WLAN-Anschlusses ein innerer

[463] LG München I, ZUM 2015, 344, 350.
[464] LG München I, ZUM 2015, 344, 350.
[465] LG München I, ZUM 2015, 344, 351.

Zusammenhang besteht.[466]

(h) Daher lautet die achte Frage, für den Fall, dass die siebte Frage verneint wird, welche zusätzlichen Kriterien an einen Diensteanbieter zu stellen sind.[467]

(i) Mit der neunten Frage will das Gericht schließlich wissen, ob es dem Access-Provider freisteht, für den Fall dass er dazu verurteilt wird, es künftig zu unterlassen, Dritten zu ermöglichen, über seinen Internetanschluss ein bestimmtes urheberrechtlich geschütztes Werk zum Abruf bereitzustellen, selbst zu bestimmen welche technischen Maßnahmen er konkret ergreift um dieser Anordnung nachzukommen.[468] Diese Frage soll vor allem unter Berücksichtigung des grundrechtlichen Schutzes des geistigen Eigentums nach Art. 17 Abs. 2 und des Grundrechts der unternehmerischen Freiheit nach Art. 16 der Charta der Grundrechte der Europäischen Union sowie der InfoSoc-RL und der Durchsetzungs-RL beantwortet werden.[469]
Weiterhin möchte das Gericht in diesem Zusammenhang wissen, ob dem Access-Provider auch eine entsprechende Anordnung auferlegt werden kann, wenn er dem gerichtlichen Verbot faktisch nur dadurch nachkommen kann, dass er entweder den Internetanschluss stilllegt oder mit einem Passwort versieht oder sämtliche über seinen Anschluss laufende Kommunikation darauf untersucht, ob das bestimmte Werk erneut urheberrechtswidrig übermittelt wird.[470]

(6) Bewertung Rechtsprechung zu gewerblichen WLAN-Anschlüssen

Zu begrüßen ist zunächst die bereits vor Einführung des WLAN-Gesetzes zunehmende Anerkennung der Privilegierung des § 8

[466] LG München I, ZUM 2015, 344, 350.
[467] LG München I, ZUM 2015, 344, 351.
[468] LG München I, ZUM 2015, 344, 351.
[469] LG München I, ZUM 2015, 344, 351.
[470] LG München I, ZUM 2015, 344, 351.

TMG auf gewerbliche Betreiber offener WLAN-Anschlüsse durch die Gerichte. Die Rechtsprechung näherte sich damit langsam der im Schrifttum seit langem herrschenden Auffassung an. Der Wortlaut des durch Umsetzung des WLAN-Gesetzes nunmehr geänderten TMG schafft diesbezüglich endlich Rechtssicherheit. Unklar ist allerdings weiterhin, ob sowohl private als auch gewerbliche WLAN-Betreiber erfasst sind. Nach der Gesetzesbegründung, die explizit Bezug nimmt auf § 2 S. 1 Nr. 1 TMG, nach dem Diensteanbieter sowohl natürliche als juristische Personen sein können[471], ist davon auszugehen, dass nach dem Willen des Gesetzgebers sowohl private als auch gewerbliche Betreiber eines WLAN-Netzes erfasst sind. Auch der Wortlaut der gesetzlichen Regelung lässt keine unterschiedliche Behandlung zu. Die Frage, ob dies auch auf europäischer Ebene der Fall ist, wird gegebenenfalls der EuGH im Laufe diesen Jahres in dem Vorabentscheidungsersuchen des LG München I beurteilen.

In den mittlerweile vorliegenden Schlussanträgen von Generalanwalt *Szpunar* geht dieser davon aus, dass Art. 12 ECRL auch für Personen gilt, die als Nebentätigkeit zu ihrer wirtschaftlichen Tätigkeit ein WLAN-Netz betreiben, das der Öffentlichkeit unentgeltlich zur Verfügung steht.[472] Es sei weder eine unmittelbare Vergütung für das Bereithalten des WLAN-Netzes notwendig noch ein aktives Anbieten oder Werben für das WLAN-Netz.[473] *Szpunar* führt zudem hinsichtlich der Sicherung des Zugangs zum öffentlichen WLAN-Netz aus, dass auch einer solchen Sicherung mehrere rechtliche Bedenken entgegenstehen.[474] Zum einen würde dies auf eine Identifizierung der Nutzer sowie eine Speicherung von Nutzerdaten hinauslaufen, was den WLAN-Betreiber als Telekommunikationsanbieter klassifizieren würde.[475] Zum anderen könnte eine entsprechende Pflicht auf eine Regelung zur Haftung des Access-Providers hinauslaufen und würde diesem

[471] BT-Drucks. 18/8645, S. 10.
[472] Szpunar, Schlussanträge vom 16. März 2016, Rn. 57.
[473] Szpunar, Schlussanträge vom 16. März 2016, Rn. 43, 53.
[474] Szpunar, Schlussanträge vom 16. März 2016, Rn. 137.
[475] Szpunar, Schlussanträge vom 16. März 2016, Rn. 140 ff.

eine aktive und präventive Rolle zuweisen, was mit der ECRL nicht mehr vereinbar wäre.[476] Insgesamt würde eine solche Verpflichtung dem Erfordernis der Herstellung eines Gleichgewichts zwischen den verschiedenen Grundrechtspositionen keine Rechnung tragen und sei für die Gesellschaft im Allgemeinen von Nachteil, so dass dieser Nachteil die möglichen Vorteile für die Urheberrechtsinhaber überwiegen könnte.[477] Ein öffentliches WLAN biete ein wichtiges Innovationspotenzial, weshalb jede Maßnahme, die diese Entwicklung bremsen könnte, gründlich auf ihren Nutzen hin zu überprüfen sei.[478]

Auf Privatpersonen, die ihr WLAN zur Verfügung stellen geht er unmittelbar nicht ein.

hh) Anwendbarkeit der Haftungsprivilegien auf Unterlassungsansprüche

Auch in Bezug auf den Access-Provider ist die Anwendbarkeit der Privilegierung auf Unterlassungsansprüche umstritten.

Fraglich ist insbesondere ob die Rechtsprechung des BGH hinsichtlich der Unanwendbarkeit im Hinblick auf Host-Provider auf den Access-Provider erstreckt werden kann.[479] Die Befürworter beziehen sich hier hauptsächlich auf § 7 Abs. 2 S. 2 TMG, welcher gleichwohl für alle Provider nach §§ 8-10 TMG gilt.[480] Insbesondere die Instanzgerichte haben die jedenfalls früher vertretene Ansicht der Unanwendbarkeit der Unterlassungsansprüche auf das Privileg des Host-Providers ohne weitergehende Prüfung auf den Access-Provider übertragen.[481]

---

[476] Szpunar, Schlussanträge vom 16. März 2016, Rn. 143 f.
[477] Szpunar, Schlussanträge vom 16. März 2016, Rn. 147 f.
[478] Szpunar, Schlussanträge vom 16. März 2016, Rn. 149.
[479] Dafür: OLG Hamburg, MMR 2009, 405, 407; LG Hamburg, ZUM 2009, 587, 589; LG Frankfurt, MMR 2008, 344, 345; Mantz/Sassenberg, MMR 2015, 85, 89; Dagegen: OLG Köln, GRUR 2104, 1081, 1089.
[480] OLG Hamburg, MMR 2014, 625, 627; OLG Hamburg, MMR 2009, 405, 407; LG Hamburg, ZUM 2009, 587, 589; LG Frankfurt, MMR 2008, 344, 345; OLG Hamburg, MMR 2004, 822, 824; Spindler, MMR 2004, 333, 334.
[481] OLG Hamburg, MMR 2009, 405, 407; LG Hamburg, ZUM 2009, 587, 589; LG Frankfurt, MMR 2008, 344, 345.

(1) „Goldesel“- und 3dl.am-Entscheidung des BGH

In zwei Urteilen hat der BGH mit nahezu wortgleicher Urteilsbegründung Anfang 2016 hinsichtlich der Verpflichtung eines Access-Providers zur Sperrung von Webseiten Stellung genommen.[482] Hier führt der I. Zivilsenat hinsichtlich der Anwendbarkeit der Privilegien zunächst aus, dass einer allgemeinen Prüfungspflicht § 7 Abs. 2 S. 1 TMG entgegenstehe, dass innerstaatliche Behörden jedoch Überwachungspflichten in spezifischen Fällen anordnen und gem. Art. 8 Abs. 3 InfoSoc-RL gerichtliche Anordnungen gegen Vermittler beantragt werden könnten.[483] Sodann formuliert der Senat, dass der Access-Provider als Dienstanbieter i.S.d. § 8 Abs. 1 S.1 TMG einzuordnen sei.[484] Ihm dürften daher keine Kontrollmaßnahmen auferlegt werden, die sein Geschäftsmodell wirtschaftlich gefährden oder seine Tätigkeit unverhältnismäßig erschweren.[485] Ohne sich weitergehend mit den spezifischen Voraussetzungen des § 8 TMG zu befassen, rezitiert der Senat schließlich den Wortlaut aus seiner „Alone in the dark“-Entscheidung[486], wonach die Auferlegung einer anlasslosen Überwachungs- oder Nachforschungspflicht nicht in Betracht komme und eine Prüfpflicht, deren Verletzung eine Wiederholungsgefahr begründen könne, erst entstehe, nachdem der Access-Provider auf eine klare Rechtsverletzung hingewiesen wurde.[487] Der Access-Provider hätte vorliegend dem anwaltlichen Schreiben, mit dem auf die Rechtsverletzungen hingewiesen wurde, nicht Folge geleistet und den Zugang zu der beanstandeten Webseite nicht unterbunden.[488] Die anlassbezogene Prüfpflicht scheiterte jedoch letzten Endes daran, dass diese für den Access-Provider nicht zumutbar gewesen sei, da der Rechteinhaber vor

[482] BGH GRUR 2016, 268 - BGH I ZR 174/14, Urteil vom 26.11.2015 – „Goldesel“; BGH MMR 2016, 188 - BGH I ZR 3/14, Urteil vom 26.11.2015 – „3dl.am“. Aufgrund der fast identischen Urteilsbegründung wird nachstehend lediglich Bezug auf das „Goldesel“-Urteil genommen.
[483] BGH GRUR 2016, 268, Rn. 21 f.
[484] BGH GRUR 2016, 268, Rn. 24.
[485] BGH GRUR 2016, 268, Rn. 27.
[486] BGH MMR 2013, 185, 189.
[487] BGH GRUR 2016, 268, Rn. 27.
[488] BGH GRUR 2016, 268, Rn. 27.

Inanspruchnahme des Access-Providers nicht jegliche zumutbare Anstrengungen unternommen habe, um gegen den Webseiten-Betreiber vorzugehen.[489]

(2) Bewertung „Goldesel"- und „3dl.am"-Entscheidung des BGH

Das Urteil des BGH hat keinerlei Klarheit in die Diskussion um die Anwendbarkeit der Privilegien auf Unterlassungsansprüche gegen den Access-Provider gebracht. Im Gegenteil, durch die unreflektierte Übernahme seiner Urteilsbegründung betreffend die Verantwortlichkeit des Host-Providers kommt es zu weiteren Ungereimtheiten. Es fragt sich, warum der erkennende Senat, nachdem er den Access-Provider bereits unter § 8 TMG subsumiert hat, nicht weiter hinsichtlich dessen Voraussetzungen ausgeführt hat. Sofern der Grund hierfür darin lag, dass der Senat den § 8 TMG nicht auf Unterlassungsansprüche anwendbar sieht, hätte er dies explizit benennen können und müssen. Die Anwendung der für den Host-Provider getroffenen Grundsätze, welche sich ohnehin bereits schwer in das Konstrukt der Haftungsprivilegien des TMG einfügen lassen, führt nunmehr zu einer Situation, die nicht nur der Haftungsprivilegierung des Access-Providers entgegensteht, sondern durch die dem Access-Provider weitere Verpflichtungen auferlegt werden. Die Rechtsprechung des BGH hinsichtlich des Host-Providers kann noch insoweit nachvollzogen werden, dass diese dahingehend im Einklang mit § 10 TMG steht, dass jedwede Haftung vor Kenntnis ausgeschlossen ist. Eine entsprechende Bezugnahme auf die Kenntnis des Access-Providers fehlt bereits in den Voraussetzungen des § 8 TMG. Das TMG knüpft insoweit nicht die Privilegierung an eine Kenntnis des Access-Providers. Dieser wird vielmehr privilegiert, sofern er die drei in § 8 TMG genannten Voraussetzungen erfüllt.

Die Störerhaftung in ihrer derzeitigen vom BGH konkretisierten Ausgestaltung ist insoweit ein Fremdkörper im Bereich der Haftungsprivilegierung des Access-Providers.

[489] BGH GRUR 2016, 268, Rn. 87.

(3) Vorabentscheidungsersuchen des LG München I

Da das Vorabentscheidungsersuchen des LG München I auch die Frage betrifft, ob Art. 12 Abs. 1 ECRL auf Unterlassungsansprüche Anwendung findet, ist eine diesbezügliche Klärung durch den EuGH zu erwarten.[490]

In den Schlussanträgen führt *Szpunar* aus, dass die Privilegierung nicht lediglich Schadensersatzansprüche gegen den Access-Provider umfasse, sondern auch sonstige Geldforderungen, die die Feststellung einer Haftung für die Verletzung eines Urheberrechts durch die Übermittlung von Informationen impliziere, wie außergerichtliche, bspw. Abmahnkosten, und gerichtliche Kosten.[491]

Es seien jedoch grundsätzlich gem. Art. 12 Abs. 3 ECRL i.V.m. Art. 8 Abs. 3 InfoSoc-RL und Art. 11 S. 3 der Durchsetzungs-RL gerichtliche Anordnungen gegen den Access-Provider möglich.[492] Diese dürften aber insbesondere nicht dazu führen, dass sie die Feststellung irgendeiner Haftung des Access-Providers für die Übermittlung von Informationen beinhalte.[493] Art. 12 ECRL skizziere insoweit gewisse Umrisse einer gerichtlichen Anordnung.[494] Zudem seien die Voraussetzungen des Art. 12 Abs. 1 ECRL abschließend, so dass ein Hinzufügen weiterer Voraussetzungen ausgeschlossen sei.[495] Entsprechend sei auch eine analoge Anwendung von Art. 14 Abs. 1 Buchst. b ECRL ausgeschlossen.[496]

Diese Ausführungen sind von grundsätzlicher Bedeutung hinsichtlich der Anwendung sowie des Umfangs der deutschen Störerhaftung mit Hinblick auf den Access-Provider und bestätigen insoweit auch die hier vertretene Ansicht hinsichtlich des Zusammenspiels von Störerhaftung und Privilegien.[497]

---

[490] LG München I, ZUM 2015, 344, 351.
[491] Szpunar, Schlussanträge vom 16. März 2016, Rn. 74.
[492] Szpunar, Schlussanträge vom 16. März 2016, Rn. 81 ff.
[493] Szpunar, Schlussanträge vom 16. März 2016, Rn. 86.
[494] Szpunar, Schlussanträge vom 16. März 2016, Rn. 87.
[495] Szpunar, Schlussanträge vom 16. März 2016, Rn. 97.
[496] Szpunar, Schlussanträge vom 16. März 2016, Rn. 104.
[497] Siehe hierzu näher S. 164.

Szpunar führt weiter aus, dass die Anordnungen fair, gerecht, nicht unnötig kompliziert oder kostspielig, wirksam, verhältnismäßig und abschreckend sein müssten.[498] Solche Anordnungen dürften zudem keine allgemeine Überwachungspflicht begründen.[499] Es seien weiterhin die entgegenstehenden Grundrechte angemessen zu berücksichtigen.[500] Grundsätzlich sei es zwar mit dem Unionsrecht vereinbar, wenn das Gericht eine Anordnung erlasse, die es dem Adressaten überlässt, die zu ergreifenden Maßnahmen zu bestimmen.[501] Allerdings müsse das Gericht sich vorher versichern, dass überhaupt eine Maßnahme existiert, die mit den unionsrechtlichen Beschränkungen im Einklang steht.[502] Generalanwalt *Szpunar* sieht die drei von dem Landgericht München I benannten Maßnahmen als nicht mit Unionsrecht vereinbar an.[503] Die gesamte Stilllegung des Internetanschlusses sei offensichtlich mit dem Erfordernis ein angemessenes Gleichgewicht zwischen den widerstreitenden Grundrechtspositionen herzustellen unvereinbar und würde einen Eingriff in den Kernbereich der unternehmerischen Freiheit bedeuten.[504] Auf den privaten WLAN-Anbieter übertragen, könnte dies einen Eingriff in die allgemeine Handlungsfreiheit darstellen.[505]

Eine Anordnung zur Überwachung der gesamten Kommunikation würde in offensichtlichem Widerspruch zu dem Verbot einer allgemeinen Überwachungspflicht stehen.[506]

Auch wenn die Schlussanträge für den EuGH nicht bindend sind, so geht von ihnen dennoch eine gewisse richtungsweisende Wirkung aus.

---

[498] Szpunar, Schlussanträge vom 16. März 2016, Rn. 108.
[499] Szpunar, Schlussanträge vom 16. März 2016, Rn. 110.
[500] Szpunar, Schlussanträge vom 16. März 2016, Rn. 111.
[501] Szpunar, Schlussanträge vom 16. März 2016, Rn. 120 unter Bezugnahme auf EuGH, GRUR 2014, 468, Rn 64.
[502] Szpunar, Schlussanträge vom 16. März 2016, Rn. 124.
[503] Szpunar, Schlussanträge vom 16. März 2016, Rn. 151.
[504] Szpunar, Schlussanträge vom 16. März 2016, Rn. 131.
[505] So auch Popescu, VuR 2011, 327, 331.
[506] Szpunar, Schlussanträge vom 16. März 2016, Rn. 132.

(4) Anwendbarkeit auf Unterlassungsansprüche nach dem neuen WLAN-Gesetz

Fraglich ist, ob sich hinsichtlich der Anwendbarkeit des § 8 TMG auf Unterlassungsansprüche durch das WLAN-Gesetz etwas geändert hat. Während der Gesetzentwurf der Bundesregierung aus November 2015 noch in einem Absatz 4 die Klarstellung enthielt, dass Diensteanbieter, die Dritten ein drahtloses Netzwerk zur Verfügung stellen, nicht auf Beseitigung oder Unterlassung in Anspruch genommen werden können, wenn sie zumutbare Maßnahmen ergriffen haben, um eine Rechtsverletzung durch einen Nutzer zu verhindern, wurde dieser Absatz im weiteren Gesetzgebungsverfahren gestrichen. Lediglich in der Gesetzesbegründung wird ausgeführt, dass die Haftungsprivilegierung des § 8 Abs. 1 und 2 TMG uneingeschränkt auch die verschuldensunabhängige Haftung im Zivilrecht nach der sog. Störerhaftung umfasst. Im Gesetz hingegen findet sich diese Anwendbarkeit auf Unterlassungsansprüche nicht wieder.

Es ist fraglich, wie der für Urheberrechtssachen zuständige I. Zivilsenat die Gesetzesbegründung zur Auslegung dieser Frage heranziehen wird. So geht der I. Zivilsenat grundsätzlich davon aus, dass für die Auslegung einer Gesetzesvorschrift der darin zum Ausdruck kommende objektive Wille des Gesetzgebers maßgeblich ist und nicht die subjektive Vorstellung der am Gesetzgebungsverfahren beteiligten Organe oder deren einzelner Mitglieder.[507] Die Auslegung hätte sich vorrangig am Sinn und Zweck des Gesetzes zu orientieren und sei nicht an Motive gebunden, die zwar im Gesetzgebungsverfahren dargelegt wurden, im Gesetzeswortlaut aber keinen Ausdruck gefunden haben.[508] Für den Fall, dass die Gesetzesbegründung jedoch zur Ermittlung des Sinn und Zwecks des Gesetzes herangezogen werden könne, könne dieser auch maßgebliche Bedeutung zur Auslegung der entsprechenden Bestimmung zukommen.[509]

[507] BGH MMR 2012, 689, 692 – Alles kann besser werden.
[508] BGH MMR 2012, 689, 692.
[509] BGH NJW-RR 2014, 354, 355 – Kindersekt.

Es ist unklar, ob der I. Zivilsenat hier von einem solchen ausdrücklich formulierten Sinn und Zweck ausgehen wird. Dagegen spricht, dass ein Vorschlag des Bundesrates zur Einfügung einer expliziten Bestimmung zur Anwendbarkeit des § 8 TMG auf Unterlassungsansprüche im weiteren Gesetzgebungsverfahren nicht weiter verfolgt wurde.[510] Da Ziel der Einführung des § 8 Abs. 3 TMG jedoch die Schaffung von Rechtssicherheit für die Anbieter von WLAN-Internetzugängen war[511], könnte allerdings argumentiert werden, dass dieses Ziel ohne eine Anwendung der Privilegien auf Unterlassungsansprüche, nicht erreicht werden kann.

(5) Ergebnis

Die Ausführungen des BGH hinsichtlich der Störerhaftung des Access-Providers in seiner „Goldesel"-Entscheidung sind abzulehnen.

Korrekterweise sind auch Unterlassungsansprüche von dem Privileg des § 8 TMG zu erfassen. Zur Begründung ist zunächst § 7 Abs. 2 S. 2 TMG sowie sein europäisches Pendant zu betrachten.

Der deutsche Gesetzgeber hat mit § 7 Abs. 2 S. 2 TMG gleich drei verschiedene Absätze der ECRL in innerstaatliches Recht umgesetzt, nämlich Art. 12 Abs. 3 ECRL, Art. 13 Abs. 2 ECRL und Art. 14 Abs. 3 ECRL.[512] Während Art. 12 Abs. 3 ECRL sowie Art. 13 Abs. 2 ECRL vom Wortlaut her identisch sind, weicht Art. 14 Abs. 3 ECRL hiervon ab. Demnach können die Mitgliedsstaaten bestimmen, dass ein innerstaatliches Gericht oder eine Verwaltungsbehörde vom Access- bzw. Cache-Provider verlangen kann, die Rechtsverletzung abzustellen oder zu verhindern. Lediglich beim Host-Provider wird dies dadurch ergänzt, dass die Mitgliedsstaaten alternativ Verfahren für die Entfernung einer Information oder die Sperrung des Zugangs zu ihr festlegen können. Im Sinn hatte der europäische Richtliniengeber hier gesetzlich vorgeschriebene *Notice and Takedown*-Verfahren, um

[510] BR-Drucks. 440/1/15.
[511] BT-Drucks. 18/8645.
[512] BT-Drucksache 14/6098, S. 23.

dem Erfordernis des Art. 14 Abs. 1 lit. b) ECRL gerecht zu werden. Da § 8 TMG allerdings nicht wie § 10 TMG eine Verpflichtung zur Sperrung und Entfernung bei Kenntnis vorschreibt, ist bei dem Access-Provider kein Platz für entsprechende Verfahren. Dementsprechend gestaltet sich auch die Begründung von Prüfpflichten und einer Nichtanwendbarkeit des § 8 TMG auf Unterlassungsansprüche schwieriger.
Möglich sind nach europäischen Vorgaben lediglich gerichtliche Anordnungen zur Entfernung bzw. Sperrung, ungeachtet einer Verantwortlichkeit des Access-Providers.
Im Übrigen greifen hier die gleichen Argumente wie bei dem Host-Provider, weshalb an dieser Stelle auf die diesbezüglichen Ausführungen verwiesen wird.[513]

ii) Fazit

Die Haftungsprivilegierung des Access-Providers hat in ihrer bisherigen Ausgestaltung durch die Rechtsprechung so gut wie keine praktische Relevanz. So wird § 8 TMG bislang weder auf WLAN-Betreiber noch augenscheinlich auf Unterlassungsansprüche angewandt. Die deutsche Rechtsprechung konzentriert sich vielmehr auf eine Verantwortlichkeit des Access-Providers im Rahmen der Störerhaftung und ignoriert damit die durch § 8 TMG geschaffene Privilegierung des Access-Providers für seine neutral vermittelnde Tätigkeit.

e) Sonstige ISP

Neben den explizit im TMG erwähnten ISP gibt es noch weitere ISP, die wichtige Funktionen im Internet wahrnehmen. Auch die ECRL erkennt die Existenz solcher ISP an. In den Schlussbestimmungen setzt Art. 21 ECRL fest, dass im Rahmen des alle zwei Jahre vorzulegenden Berichts der Kommission über die Anwendung der Richtlinie auch das etwaige Erfordernis einer Anpassung der ECRL im Hinblick auf die Haftung von Anbietern

[513] Siehe S. 79.

von Hyperlinks und von Instrumenten zur Lokalisierung von Informationen untersucht werden soll.

Im Folgenden wird lediglich in dem Maße auf die bisherig ergangene Rechtsprechung Bezug genommen, wie dies für das Aufzeigen von Parallelen dieser Rechtsprechung zu den Haftungsprivilegien der anderen ISP von Interesse ist.

aa) Anbieter von Hyperlinks

Anbieter von Hyperlinks sind von den Privilegien ausgenommen und unterliegen damit einer Haftung nach den allgemeinen Gesetzen.[514] Unter den weiten Begriff der Anbieter von Hyperlinks können sowohl Nutzer fallen, die Links auf Webseiten setzen, Suchmaschinen, die Links für Nutzer auf deren Anfrage bereitstellen, und sonstige Diensteanbieter, die Hyperlinks zu fremden Inhalten bereitstellen.

Für den Bereich des Urheberrechts hat der BGH bereits 2003 geurteilt, dass das Setzen eines Hyperlinks keine täterschaftliche Verletzung des Vervielfältigungsrechts bzw. des Rechts der öffentlichen Zugänglichmachung darstellt.[515]

Der Link stellt lediglich eine elektronische Verknüpfung dar, durch welche es weder zu einer urheberrechtlich relevanten Vervielfältigung noch zu einer öffentlichen Zugänglichmachung kommt.[516] Zu einer Vervielfältigung kann es erst kommen, wenn der Nutzer den Link anklickt um eine Datei abzurufen.[517] Eine öffentliche Zugänglichmachung hat derjenige vorgenommen, der das Werk ursprünglich ins Internet gestellt hat, die Verlinkung verweist lediglich auf das Werk in einer Weise, die Nutzern den bereits eröffneten Zugang erleichtert.[518]

Entsprechend ist auch bei der Verlinkung auf urheberrechtlich zulässige Inhalte eine Störerhaftung des Verlinkenden zu verneinen da es hier bereits an einer Verletzung urheberrechtlicher

[514] BT-Drucksache 14/6098, S. 37.
[515] BGH GRUR 2003, 958 – „Paperboy“.
[516] BGH GRUR 2003, 958, 961 f.
[517] BGH GRUR 2003, 958, 961.
[518] BGH GRUR 2003, 958, 962.

Nutzungsrechte fehlt.[519] Dies gilt jedenfalls dann, wenn ein urheberrechtlich geschütztes Werk ohne technische Schutzmaßnahmen im Internet öffentlich zugänglich gemacht wird.[520]

Erfolgt eine Verlinkung indes auf urheberrechtswidrige Inhalte, so hängt eine Haftung des Linksetzenden von der Kenntnis der Rechtswidrigkeit bzw. der Verletzung von Prüfpflichten ab.[521] Verletzt der Linksetzende zumutbare Prüfpflichten, kommt eine Haftung als Störer in Betracht. Der Umfang der Prüfpflichten richtet sich nach dem Gesamtzusammenhang, in dem der Hyperlink verwendet wird, dem Zweck des Hyperlinks sowie danach, welche Kenntnis der Linksetzende von Umständen hat, die dafür sprechen, dass der verlinkte Inhalt rechtwidrig ist und welche Möglichkeiten er hat, diese Rechtswidrigkeit in zumutbarer Weise zu erkennen.[522]

Der BGH hat zudem mit seinem letzten Urteil „Haftung für Hyperlinks“[523] explizit die Maßstäbe des TMG auf Linksetzende übertragen sowie seine Argumentationslinie hinsichtlich der Haftung des Host-Providers mit der des Linksetzenden in Einklang gebracht. So führt er aus, dass zur Konkretisierung der Prüfpflichten auf die vom Senat im Zusammenhang mit Host-Providern entwickelten Grundsätze zurückgegriffen werden könne.[524] Obwohl für Linksetzende die Privilegien des TMG nicht griffen, sei es dennoch gerechtfertigt diesen keine proaktive Überwachungspflicht aufzuerlegen, da Hyperlinks für die Internetnutzer unerlässlich seien, um die unübersehbare Informationsflut des Internets zu erschließen.[525] Daher würde der Linksetzende, sofern der rechtsverletzende Inhalt der verlinkten Webseite nicht deutlich erkennbar sei, für solche Inhalte grundsätzlich erst dann haften, wenn Dritte ihn über die

[519] BGH GRUR 2003, 958, 961.
[520] BGH GRUR 2003, 958, 961.
[521] So bereits BGH GRUR 2004, 693 für den Bereich des illegalen Glücksspiels.
[522] BGH GRUR 2004, 693, 695.
[523] BGH GRUR 2016, 209.
[524] BGH GRUR 2016, 209, 212.
[525] BGH GRUR 2016, 209, 212.

Rechtswidrigkeit in Kenntnis setzten.[526] Allerdings sei, anders als beim Host-Provider, keine klare Rechtsverletzung zu verlangen, sondern den Linksetzenden treffe nach entsprechendem Hinweis eine Prüfung der verlinkten Internetseite, auch wenn es sich nicht um eine klar erkennbare Rechtsverletzung handele.[527] Als Begründung für diese Ungleichbehandlung des Linksetzenden ggü. dem Host-Provider führte der erkennende Senat die unterschiedliche Interessenlage an. Während es sich bei dem Host-Provider um ein von der Rechtsordnung gebilligte Geschäftsmodell handele, würden Hyperlinks auf kommerziellen Webseiten diesen lediglich ein zusätzliches Informationsangebot hinzufügen, das für die auf dieser Webseite angebotenen Waren oder Dienstleistungen weder essenziell wäre noch ihren Wert oder Nutzen steigere.[528] Da es sich zudem zumeist um eine begrenzte Anzahl von Hyperlinks auf der Webseite handele, sei es daher sachgerecht, das Risiko einer rechtlichen Beurteilung der verlinkten Inhalte dem Linksetzenden zuzuordnen.[529]

Je nach konkreter Ausgestaltung der Linksetzung kann die fremde Information, auf die der Hyperlink verweist, dem Linksetzenden zudem als eigene Information zugerechnet werden.[530]

bb) Suchmaschinen-Anbieter

Auch die Tätigkeit des Suchmaschinen-Anbieters unterliegt nicht den Privilegierungen des TMG.

Bei der Bewertung des potentiellen Haftungsrisikos des Suchmaschinen-Anbieters ist jedoch zwischen den verschiedenen Funktionen, welche der Suchmaschinen-Anbieter ausführt, zu unterscheiden.

(1) Anzeigen von Ergebnislisten auf Suchanfrage

Zunächst einmal ist da die typische Tätigkeit des Suchmaschinen-Anbieters, welche in der Zurverfügungstellung von Hyperlinks

[526] BGH GRUR 2016, 209, 212.
[527] BGH GRUR 2016, 209, 212 f.
[528] BGH GRUR 2016, 209, 212 f.
[529] BGH GRUR 2016, 209, 213.
[530] Siehe BGH GRUR 2008, 534, 536 für den Bereich des Wettbewerbsrechts.

aufgrund der zuvor getätigten Suchanfrage des Nutzers besteht. In dieser Hinsicht bemisst sich eine etwaige Verantwortlichkeit des Suchmaschinen-Anbieters nach den gleichen Grundsätzen wie die des Linksetzers. Dies gilt auch bei der Anzeige sog. Snippets, das sind kurze Textauszüge aus einer Webseite, die in der Ergebnisliste einer Suchmaschine angezeigt werden.[531]

Im Gegensatz zum „bloßen" Linksetzer ist bei dem Suchmaschinen-Anbieter aber insbesondere bei der Bewertung von dessen Prüfpflichten dessen Schlüsselfunktion für das Auffinden von Inhalten im Internet zu beachten.[532] Aufgrund der automatischen Generierung und Anzeige einer riesigen Anzahl von Suchergebnissen ist der Suchmaschinenanbieter grundsätzlich nicht dazu verpflichtet, die durch eine Suchanfrage generierten Links auf rechtswidrige Inhalte zu überprüfen.[533] Entsprechend ist er auch nicht als Störer haftbar. Eine Prüfpflicht trifft den Suchmaschinen-Anbieter allerdings sofern dieser ganz konkret auf eine Urheberrechtsverletzung hingewiesen wurde, so dass dieser die Möglichkeit hat, diese aus seiner Ergebnisliste zu entfernen.[534]

Das *LG Hamburg* hält es für den Suchmaschinen-Anbieter anscheinend sogar für zumutbar, Maßnahmen zu ergreifen, um zukünftige Rechtsverletzungen des Berechtigten zu verhindern.[535] Was diese Verpflichtung für den Suchmaschinen-Anbieter genau beinhaltet, führt das Gericht allerdings nicht weiter aus.

(2) Anzeigen von Vorschaubildern in Ergebnislisten

Das „Vorschaubilder I"-Urteil des I. Zivilsenats behandelte die textgesteuerte Bildsuchfunktion von Google, bei der der Nutzer durch Eingabe eines Suchbegriffes nach Abbildungen suchen kann, die Dritte im Zusammenhang mit dem eingegeben Suchwort ins

[531] KG, MMR 2012, 129; OLG Hamburg, MMR 2011, 685; Söder in BeckOK InfoMedienR, § 823 BGB, Rn. 26.
[532] Spindler/Volkmann in Spindler/Schuster, § 1004 BGB, Rn. 49.
[533] OLG Hamburg, MMR 2011, 685, 687; OLG Nürnberg, MMR 2009, 131, 132; Reber in BeckOK UrhG, § 97 Rn. 78.
[534] OLG München, MMR 2012, 108, Reber in BeckOK, UrhG, § 97 Rn. 78; Söder in BeckOK InfoMedienR, § 823 BGB, Rn. 25.
[535] LG Hamburg, NJW 2015, 796, 801.

Internet gestellt haben.[536] Die von der Suchmaschine aufgefundenen Bilder werden in der Trefferliste in verkleinerter und in ihrer Pixelzahl reduzierten Form angezeigt. Der BGH führt hier zunächst aus, dass durch die Anzeige in der Trefferliste in das Recht des Urhebers auf Vervielfältigung und öffentlichen Zugänglichmachung eingegriffen werde.[537] Allerdings sieht er in der Tatsache, dass der Urheber bei der Einstellung des Bildes ins Internet ohne eine entsprechende Blockierung von Suchmaschenindexierungen eine schlichte Einwilligung des Rechteinhabers, weshalb der Eingriff nicht rechtswidrig sei.[538]
In einem obiter dictum weist der erkennende Senat zudem darauf hin, dass für den Fall, dass das Bild ohne Zustimmung des Rechteinhabers ins Internet gestellt wurde, könne zwar nicht auf eine Einwilligung seitens des Rechteinhabers geschlossen werden, es käme hier aber in Betracht, die Haftung auf solche Verstöße zu beschränken, die nach Hinweis auf eine klare Rechtsverletzung begangen werden.[539] Eine solche Möglichkeit der Haftungsbeschränkung für die Bereitstellung von Informationen in Suchmaschinen für den Zugriff durch Dritte ergebe sich aus Art. 14 Abs.1 ECRL.[540]

(3) Autocomplete-Funktion

Bei der Autocomplete-Funktion handelt es sich um eine Funktion innerhalb der Suchmaschine, die, sobald der Nutzer anfängt einen Suchbegriff einzugeben, auf der Basis eines Algorithmus automatisch verschiedene Suchvorschläge in Form von Wortkombinationen ermittelt und diese in einem sich daraufhin öffnenden Fenster anzeigt.[541] Der Algorithmus basiert dabei nach Angabe von Google auf zuvor von Nutzern getätigten Suchanfragen.

[536] BGH GRUR 2010, 628.
[537] BGH GRUR 2010, 628, 629.
[538] BGH GRUR 2010, 628, 632.
[539] BGH GRUR 2010, 628, 633.
[540] BGH GRUR 2010, 628, 633.
[541] Siehe Sachverhaltsbeschreibung in BGH GRUR 2013, 751.

Obwohl diese Funktion für den Bereich des Urheberrechts keine Bedeutung erlangt, da durch die Autocomplete-Funktion keine Urheberrechte verletzte werden sondern es vielmehr zu Persönlichkeitsrechtsverletzungen kommen kann, wird im Folgenden kurz die höchstrichterliche Rechtsprechung im Hinblick auf die Verantwortlichkeit des Suchmaschinen-Anbieters für persönlichkeitsrechtsverletzende Begriffsverbindungen durch die Autocomplete-Funktion darstellt werden. Dies ist insbesondere vor dem Hintergrund von Interesse, dass der erkennende Senat sich eng an den Grundsätzen der Haftung des Host-Providers orientiert hat.

Der VI. Zivilsenat hat entschieden, dass die von dem Suchmaschinen-Anbieter angezeigten Suchvorschläge im Rahmen der Autocomplete-Funktion als eigene Inhalte des Suchmaschinen-Anbieters zu qualifizieren sind.[542] Er sei demnach nach den allgemeinen Gesetzen für diese Suchvorschläge verantwortlich.[543]

Der Senat lässt den Suchmaschinen-Anbieter für diese eigenen Inhalte dennoch lediglich im Umfang der Störerhaftung haften und setzt auch hier die Verletzung von Prüfpflichten voraus.[544] Er begründet dies damit, dass der Schwerpunkt der Vorwerfbarkeit des Suchmaschinen-Anbieters in einem Unterlassen liegt.[545] Bei der Verwendung der Autocomplete-Funktion durch den Suchmaschinen-Betreiber handele es sich um eine durch Art. 2 und Art. 14 GG geschützte wirtschaftliche Tätigkeit, welche nicht von vornherein auf eine Rechtsverletzung abziele.[546] Lediglich durch das Hinzutreten eines gewissen Nutzerverhaltens können ehrverletzende Begriffsverbindungen entstehen.[547]

Der Suchmaschinen-Anbieter sei deshalb gehalten, nachdem er von dem Betroffenen hinsichtlich einer rechtwidrigen Verletzung seines

[542] BGH GRUR 2013, 751, 752.
[543] BGH GRUR 2013, 751, 752.
[544] BGH GRUR 2013, 751, 753 f.
[545] BGH GRUR 2013, 751, 753.
[546] BGH GRUR 2013, 751, 753.
[547] BGH GRUR 2013, 751, 753.

Persönlichkeitsrechts in Kenntnis gesetzt wird, zukünftig derartige Verletzungen zu verhindern.[548]

(4) Fazit

Eine Störerhaftung des Linksetzenden und Suchmaschinen-Anbieters ist grundsätzlich erst nach konkreter Kenntnis des rechtsverletzenden Inhaltes denkbar. Erst dann kann ihn unter bestimmten Umständen die Pflicht treffen, bzgl. des konkreten Inhaltes tätig zu werden. Damit steht die Rechtsprechung grundsätzlich im Einklang mit der zur Verantwortlichkeit der ISP im Sinne des TMG entwickelten Rechtsprechung. Irritierend sind insoweit die nebenbei gemachten Ausführungen des I. Zivilsenats, dass im Rahmen der Anzeige von Vorschaubildern durch Google auch eine Haftungsprivilegierung nach Art. 14 Abs. 1 ECRL in Betracht komme, zumal er sich hier auf ein Urteil des EuGH im Rahmen der Werbung mit AdWords bezieht.

Eine Anlehnung der Haftungsprivilegierung des Linksetzenden und Suchmaschinen-Anbieters an die Vorgaben des TMG ist jedoch grundsätzlich zu begrüßen. Da die Verlinkung von Inhalten im Internet von großer gesellschaftlicher Bedeutung ist, wäre eine explizite gesetzliche Regelung auf europäischer Ebene allerdings wünschenswert. Eine entsprechende Regelung würde im Idealfall auch für solche Diensteanbieter das erforderliche Maß an Rechtssicherheit bringen und eine einheitliche Handhabung in den Mitgliedstaaten sicherstellen. Es ist nicht klar, warum Anbieter von Suchmaschinen-Services diesbezüglich gegenüber anderen ISP benachteiligt werden sollten.

6. Ergebnis

Wie sich gezeigt hat, spielen die gesetzlichen Privilegierungstatbestände nur eine untergeordnete Rolle in der Rechtssprechungspraxis. Die Gerichte orientieren sich zur Bestimmung der Haftung der ISP vornehmlich an den allgemeinen

[548] BGH GRUR 2013, 751, 754.

Gesetzen. Dass dies im Sinne des europäischen bzw. deutschen Gesetzgebers ist, darf zurecht bezweifelt werden.

II. Verantwortlichkeit für Urheberrechtsverletzungen nach den allgemeinen Gesetzen

Eine Anwendbarkeit der allgemeinen Gesetze kommt in zwei unterschiedlichen Konstellationen in Betracht. Zunächst ist eine Verantwortlichkeit der ISP im Rahmen der allgemeinen Gesetze zu beurteilen, sofern diese aus dem Anwendungsbereich des TMG herausfallen. Zudem kommen auch im Falle einer Privilegierung nach dem TMG Verpflichtungen zur Entfernung und Sperrung nach den allgemeinen Gesetzen in Betracht.

1. Zivilrechtliche Verantwortlichkeit des Host-Providers

Für die zivilrechtliche Verantwortlichkeit des Host-Providers kommen unterschiedliche Beteiligungsformen in Betracht.

a) Täter/Teilnehmer

Die Frage, ob jemand Täter, Mittäter, Anstifter oder Gehilfe in einer die zivilrechtliche Haftung begründeten Weise an einer deliktischen Handlung eines Dritten beteiligt ist, beurteilt sich nach den im Strafrecht entwickelten Rechtsgrundsätzen.[549]

aa) Täter

Verletzer eines Urheberrechts ist zunächst, wer selbst als Täter oder in Mittäterschaft ein nach dem Urheberrecht geschütztes Recht verletzt.[550] Im Falle des Host-Providers wird dieser aber die Verletzungshandlung, also die Vervielfältigung und öffentliche Zugänglichmachung durch den Upload der Datei, nicht selbst vorgenommen haben. Eine Haftung des Host-Providers als Täter scheidet daher im Regelfall aus.[551]

Denkbar wäre jedoch eine Haftung als Täter durch ein „zu eigen machen“ der Inhalte Dritter. Der I. Zivilsenat hat ein solches zu

[549] BGH MMR 2011, 172, 173.
[550] Reber in BeckOK UrhG, § 97 Rn. 35.
[551] So auch BGH MMR 2013, 185, 185.

eigen Machen im Fall „marions.kochbuch.de“ aufgrund einer redaktionellen Kontrolle sowie einer sichtbar nach außen tretenden inhaltlichen Verantwortung für die Inhalte bejaht.[552]

bb) Teilnehmer

Als Teilnehmer haftet derjenige, der entweder als Anstifter oder Gehilfe zu einer Urheberrechtsverletzung beiträgt.

Anstifter ist im Sinne des § 26 StGB derjenige, der einen anderen vorsätzlich zu dessen vorsätzlich begangenen rechtswidrigen Tat bestimmt hat. Beihilfe im Sinne des § 27 StGB leistet derjenige, der vorsätzlich einem anderen zu dessen vorsätzlich begangenen rechtswidrigen Tat Hilfe geleistet hat. Auch eine Beihilfe durch Unterlassen im Sinne des § 13 StGB ist möglich.[553]

Dabei bedarf es eines Gehilfenbeitrags in dem Zeitraum vom Vorbereitungsstadium der Tat bis zur Vollendung der Tat.[554]

Bei dem rechtswidrigen Hochladen einer urheberrechtlich geschützten Datei ist die maßgebliche Tathandlung die öffentliche Zugänglichmachung gem. § 19a UrhG.

Der Tatbestand der öffentlichen Zugänglichmachung ist zwar zunächst erfüllt, sofern das Werk derart im Internet oder sonstigen Netzwerken zugänglich gemacht wird, dass Dritten der Zugriff hierauf eröffnet wird. Es handelt sich in diesem Fall jedoch um ein Dauerdelikt, da der rechtswidrige Zustand bei der öffentlichen Zugänglichmachung einer urheberrechtlich geschützten Datei durch deren Bereitstellung auf dem Server des Host-Providers auch nach dem Hochladen der Datei aufrechterhalten wird.[555]

Eine Beihilfe ist somit solange möglich, wie die Datei auf dem Server des Host-Providers zum Abruf bereit steht.

Die Teilnahme an einer Urheberrechtsverletzung erfordert weiterhin einen doppelten Vorsatz, d.h. der Vorsatz muss sich sowohl auf die Haupttat als auch die Tathandlung des Anstifters

[552] BGH GRUR 2010, 616.
[553] BGH MMR 2011, 172, 173.
[554] Kudlich in BeckOK StGB, § 27 Rn. 7.
[555] BGH ZUM-RD 2011, 296, 297; LG München I ZUM-RD 2015, 118, 121.

bzw. Gehilfen beziehen.[556] Erforderlich ist mindestens bedingter Vorsatz, der das Bewusstsein der Rechtswidrigkeit einschließen muss.[557]

An diesen Voraussetzungen dürfte es im Normalfall beim Host-Provider fehlen. Der Host-Provider stellt in seiner Funktion als Diensteanbieter lediglich Speicherplatz für einen Dritten zur Verfügung. Er hat in der Regel keine Kenntnis bezüglich der Inhalte, die der Dritte auf diesem Speicherplatz bereithält sowie keinen Einfluss hierauf. Deshalb ist seine Tätigkeit als sozial nützliche und erwünschte Tätigkeit gem. § 10 TMG privilegiert. Dieses Privileg verliert der Host-Provider erst, wenn er Kenntnis von der Urheberrechtsverletzung erlangt und nach Kenntnis nicht tätig wird.

So hat der BGH hinsichtlich einer Markenrechtsverletzung auf einer Internetplattform ausgeführt, dass der Host-Provider selbst nicht die markenrechtsverletzende Ware angeboten habe und auch nicht bewusst und gewollt mit den Verletzern zusammenwirke, sofern er lediglich seine Plattform Dritten zur Verfügung stelle.[558] Er erlange durch das automatisierte Verfahren keine vorherige Kenntnis von der Rechtsverletzung, weshalb auch ein vorsätzliches Zusammenwirken mit dem Verletzer ausscheide.[559]

(1) Anstifter

Eine Haftung des Host-Providers als Anstifter kommt in Betracht, wenn der Host-Provider durch Einwirkung auf den Willen eines Dritten bei diesem einen Tatentschluss hervorruft.[560] Denkbar wäre dies in Fällen, in denen der Host-Provider die Popularität seines Dienstes, bspw. einer Videoplattform, dadurch steigern will, dass er Dritte darum bittet, urheberrechtswidriges Material dort hochzuladen. Der Host-Provider würde hier sowohl hinsichtlich

[556] Dölling/Duttge/Rössner, Gesamtes Strafrecht, § 27 StGB, Rn. 18.
[557] BGH GRUR 2011, 152, 154; Dölling/Duttge/Rössner, Gesamtes Strafrecht, § 27 StGB, Rn. 18.
[558] BGH MMR 2011, 172, 173.
[559] BGH MMR 2011, 172, 173.
[560] Kudlich in BeckOK StGB, § 26 Rn. 12.

seiner Tathandlung als auch der Haupttat des Dritten vorsätzlich handeln.

(2) Gehilfe

Der Host-Provider könnte durch Hilfeleistung zur Haupttat eines Dritten als Gehilfe haften.

Für die Annahme eines Gehilfenvorsatzes genügt es jedoch nicht, wenn der Diensteanbieter mit gelegentlichen Rechtsverletzungen rechnet, dieser muss sich vielmehr auf die konkret drohende Haupttat beziehen.[561]

Es käme allerdings eine Beihilfe durch Unterlassen in Betracht. Voraussetzung hierfür ist, dass eine Rechtspflicht zum Handeln bestand.[562]

(a) Urteil des OLG Hamburg

Das OLG Hamburg hat bislang als einziges Gericht eine Gehilfenhaftung des Host-Providers bejaht.[563] In dem Fall ging es um einen File-Hosting-Dienst, welcher trotz mehrfacher Hinweise eines Rechteinhabers auf eine Urheberrechtsverletzung die entsprechende Datei nicht löschte oder sperrte. Das Gericht führte zunächst aus, dass eine Privilegierung nach § 10 TMG nicht in Betracht komme, da der Host-Provider nicht, wie von § 10 Satz 1 Nr. 2 TMG vorgeschrieben, nach Kenntnis über die Rechtsverletzung unverzüglich tätig geworden sei.[564]

Eine Haftung sei folglich nach den allgemeinen Grundsätzen zu bewerten, im konkreten Fall die Haftung als Gehilfe.[565]

Die objektive Unterstützungshandlung sah das Gericht bei der Zurverfügungstellung von verlinkbarem Speicherplatz, welcher die Urheberrechtsverletzung überhaupt erst möglich gemacht hätte, sowie der daran anschließenden Duldung der Rechtsverletzung trotz Kenntnis.[566]

---

[561] BGH GRUR 2007, 708, 710.
[562] Heine/Weißer in Schönke/Schröder, § 27 Rn. 19.
[563] OLG Hamburg, MMR 2013, 533.
[564] OLG Hamburg, MMR 2013, 533, 533.
[565] OLG Hamburg, MMR 2013, 533, 534.
[566] OLG Hamburg, MMR 2013, 533, 534.

Dass der doppelte Gehilfenvorsatz noch nicht beim Hochladen der Datei vorlag, sei unerheblich, da dem Host-Provider nicht ein positives Tun, sondern ein Unterlassen vorgeworfen werde.[567]

Nach Kenntnis der Rechtsverletzung hätte der Host-Provider im Hinblick auf die Haupttat mit bedingtem Vorsatz gehandelt und das Andauern der Rechtsverletzung billigend in Kauf genommen.[568]

Durch das hartnäckige Ignorieren der Hinweise lag bei dem Host-Provider auch im Hinblick auf seine eigene Tathandlung bedingter Vorsatz vor.[569]

Die Rechtspflicht, den Erfolg abzuwenden, läge in der zuvor den Host-Provider treffenden Störerhaftung, welche den Host-Provider verpflichte, nach Kenntnis den Zugang zu der Datei zu sperren.[570]

Das Gericht weist schließlich nochmals darauf hin, dass nicht jede nicht unverzügliche Sperrung zu einer Gehilfenhaftung führe, sondern lediglich die hartnäckige Weigerung, die andauernde Rechtsverletzung zu beenden.[571]

(b) Bewertung

Auch der BGH hat jedenfalls die potentielle Möglichkeit einer Gehilfenhaftung in Folge der nachhaltigen Pflichtverletzung des Störers gesehen, die Beantwortung dieser Frage allerdings offen gelassen.[572]

Fraglich ist, ob den Host-Provider überhaupt eine Garantenpflicht trifft. Die Garantenpflicht ist eine rechtliche Handlungspflicht, welche voraussetzt, dass der Garant dafür einzustehen hat, dass ein bestimmter Erfolg nicht eintritt.[573] Sie kann sich aus Gesetz oder Vertrag ergeben oder auf vorangegangenem gefährdenden Tun oder enger Lebensgemeinschaft beruhen.[574]

Aus § 10 S. 1 Nr. 2 TMG kann keine Garantenpflicht abgeleitet werden. Das TMG setzt lediglich die Voraussetzungen für eine

[567] OLG Hamburg, MMR 2013, 533, 534.
[568] OLG Hamburg, MMR 2013, 533, 534.
[569] OLG Hamburg, MMR 2013, 533, 534.
[570] OLG Hamburg, MMR 2013, 533, 534.
[571] OLG Hamburg, MMR 2013, 533, 534.
[572] BGH MMR 2004, 668, 671.
[573] Heuchemer in BeckOK StGB, § 13 Rn. 33.
[574] Heuchemer in BeckOK StGB, § 13 Rn. 34.

Privilegierung des Host-Providers fest, begründet aber keine Pflichten auf Seiten des Host-Providers. Sofern der Host-Provider die beanstandeten Inhalte nicht gem. § 10 S. 1 Nr. 2 TMG entfernt bzw. sperrt, fällt er lediglich aus dem Anwendungsbereich des § 10 TMG heraus und seine Verantwortlichkeit bestimmt sich nach den allgemeinen Gesetzen.

Denkbar ist daher eine Garantenpflicht aus den sich aus der Störerhaftung ergebenden Prüfpflichten.

Sofern der Host-Provider Kenntnis von einer Rechtsverletzung hat und diese nicht unverzüglich entfernt bzw. sperrt, ist er nicht mehr von § 10 TMG privilegiert und kann somit auch als Störer haften.

Die Haftung des Störers setzt die Verletzung von Prüfungspflichten voraus, deren Umfang sich danach bestimmt, ob und inwieweit dem Störer eine Prüfung zuzumuten ist.

Ihn trifft folglich eine Handlungspflicht, um einer Inanspruchnahme als Störer für die Verletzung eines Urheberrechts zu entgehen. Das OLG Hamburg leitet aus dieser Pflicht eine Garantenstellung des Host-Providers ab, so dass bei deren Verletzung der Host-Provider als Gehilfe durch Unterlassen haftet.[575]

Dieser Ansicht wird zu Recht entgegengehalten, dass dadurch jeder Störer automatisch eine Beihilfe durch Unterlassen begehen würde, da es für die Garantenpflicht ausreichen würde, die Voraussetzungen der Störerhaftung zu erfüllen.[576]

Zudem müsste sich eine ggf. zu erwägende Garantenstellung an § 7 Abs. 2 S. 1 TMG orientieren, das heißt, sie darf dem Host-Provider keine allgemeine Überwachungspflicht auferlegen.[577]

Eine derartige Einordnung der Prüfpflichten im Rahmen der Störerhaftung ist nicht geboten. Dies ergibt sich bereits aus der ursprünglichen Begründung derartiger Prüfpflichten. Die Störerhaftung legt einem Dritten, welcher selbst nicht die

[575] OLG Hamburg, MMR 2013, 533, 534. So auch Ensthaler/Heinemann, GRUR 2012, 433, 440.
[576] Rempe, MMR 2013, 533, 534.
[577] Ensthalter/Heinemann, GRUR 2012, 433, 434.

Rechtsverletzung begangen hat oder an dieser beteiligt war, sondern lediglich adäquat kausal an der Herbeiführung oder Aufrechterhaltung einer Urheberrechtsverletzung mitgewirkt hat, eine Beseitigungs- und Unterlassungsverpflichtung auf.[578] Prüfpflichten wurden in diesem Zusammenhang lediglich eingeführt, um die Haftung von Dritten nicht über Gebühr auszudehnen.[579] Die Prüfpflichten sind folglich ein Instrument zur Einschränkung der Haftung des Dritten. Würde man hieraus nun eine Garantenstellung des Host-Providers ableiten, so würde dies dem ursprünglichen Sinn und Zweck der Einführung zumutbarer Prüfpflichten im Rahmen der Störerhaftung klar zuwiderlaufen.
Eine Garantenstellung des Host-Providers ist folglich abzulehnen.

(c) Rechtsprechung des BGH

In der Entscheidung „Kinderhochstühle im Internet I“[580] setzte sich auch der BGH mit der Frage der Beihilfe des Host-Providers auseinander. Das Berufungsgericht hatte hier eine Beihilfe des Plattformbetreibers durch Unterlassen zur Markenrechtsverletzung eines Dritten gesehen, da diesen zur Verhinderung von Rechtsverletzungen bereits vor der Veröffentlichung von Angeboten auf seiner Plattform Prüfungspflichten träfen.[581]
Der BGH folgte dem nicht und führte hinsichtlich der Beihilfe durch Unterlassen aus, dass diese zusätzlich zur objektiven Unterstützung der Rechtsverletzung, dem Vorsatz in Bezug auf die Haupttat und dem Bewusstsein der Rechtswidrigkeit voraussetze, dass den Gehilfen eine Rechtspflicht treffe, den Erfolg abzuwenden.[582] Der erkennende Senat hat allerdings offen gelassen, ob den Host-Provider hier überhaupt eine Erfolgsabwendungspflicht trifft, da er diese jedenfalls nicht verletzt habe.[583] Eine manuelle Kontrolle von denen durch eine

[578] v. Wolff in Wandtke/Bullinger, § 97, Rn. 15.
[579] BGH GRUR 2001, 1038, 1039.
[580] BGH MMR 2011, 172.
[581] OLG Hamburg, NJOZ 2008, 4082.
[582] BGH MMR 2011, 172, 173.
[583] BGH MMR 2011, 172, 173.

Filtersoftware aufgedeckter Verdachtsfälle, sei dem Host-Provider nach Abwägung der wechselseitigen Interessen nicht zumutbar.[584]
Ebenfalls nicht ausreichend für den erforderlichen Gehilfenvorsatz sei es, wenn der Host-Provider mit gelegentlichen Rechtsverletzungen der Nutzer auf seiner Plattform rechne, erforderlich sei vielmehr die Kenntnis von der konkret drohenden Haupttat.[585]

(d) Zwischenergebnis

Eine Haftung des Host-Providers als Gehilfe nach erfolgter öffentlicher Zugänglichmachung einer urheberrechtswidrigen Information durch den Täter ist unwahrscheinlich. Eine Garantenpflicht im Rahmen der Störerhaftung ist nicht gegeben, so dass eine Beihilfe wegen Unterlassung aufgrund einer Verletzung der Prüfpflichten ausscheidet.
Denkbar ist daher allenfalls eine Beihilfe beispielsweise durch vorsätzliches Hinwirken auf die Nutzer seines Dienstes, beispielsweise durch offensive Werbung für das Hochladen urheberrechtswidriger Inhalte.[586]

cc) Rechtsfolgen

Für den Fall, dass den Host-Provider eine Verantwortlichkeit als Täter oder Teilnehmer trifft, kann der Berechtigte die folgenden Ansprüche ihm gegenüber geltend machen.

(1) Beseitigungs- und Unterlassungsanspruch, § 97 Abs. 1 UrhG

Gemäß § 97 Abs. 1 UrhG kann, wer das Urheberrecht widerrechtlich verletzt, von dem Verletzten auf Beseitigung der Beeinträchtigung, bei Wiederholungsgefahr auf Unterlassung in Anspruch genommen werden. Der Anspruch auf Unterlassung besteht nach § 97 Abs. 1 S. 2 UrhG auch dann, wenn eine Zuwiderhandlung erstmalig droht.

---

[584] BGH MMR 2011, 172, 174.
[585] BGH MMR 2013, 185, 186.
[586] So auch Spindler, MMR 2006, 403, 404; vom BGH offen gelassen in BGH, GRUR 2009, 841, 843.

Eine widerrechtliche Verletzung des Urheberrechts ist dann gegeben, wenn entweder das Urheberpersönlichkeitsrecht oder die Verwertungsrechte des Urhebers verletzt werden.

Im Falle des Host-Providers, der Dritten Speicherplatz zur Verfügung stellt, wird die gegenständliche Verletzungshandlung die unberechtigte Vervielfältigung gem. § 16 UrhG sowie das Recht der öffentlichen Zugänglichmachung gem. § 19a UrhG betreffen. Der Eingriff in dieses Recht begründet bereits die Vermutung der Rechtswidrigkeit.[587] Die Beweislast, dass der Eingriff rechtmäßig erfolgt ist, bspw. da eine Einwilligung des Rechteinhabers vorliegt, trifft daher den Verletzer.[588]

Während für den Beseitigungsanspruch lediglich eine fortdauernde Beeinträchtigung verlangt wird, ist weitere Voraussetzung für den Unterlassungsanspruch das Bestehen einer Wiederholungsgefahr.[589] Die Wiederholungsgefahr wird regelmäßig durch eine bereits begangene Rechtsverletzung indiziert.[590]

(2) Schadensersatzanspruch, § 97 Abs. 2 UrhG

Wer das Urheberrecht vorsätzlich oder fahrlässig widerrechtlich verletzt ist gem. § 97 Abs. 2 UrhG dem Verletzten zum Ersatz des daraus entstanden Schadens verpflichtet.

Anders als der Unterlassungs- und Beseitigungsanspruch setzt der Schadensersatzanspruch ein Verschulden des Host-Providers voraus.

Ein Verschulden ist im Bereich der Täter-/Teilnehmerhaftung regelmäßig gegeben.

b) Störer

Als Störer haftet nach ständiger Rechtsprechung derjenige, der ohne Täter oder Teilnehmer zu sein, in irgendeiner Weise willentlich und adäquat kausal zur Verletzung eines geschützten Rechtsguts beiträgt.[591] Damit sich die Störerhaftung nicht über

[587] Reber in BeckOK UrhG, § 97 Rn. 84.
[588] Reber in BeckOK UrhG, § 97 Rn. 84.
[589] Reber in BeckOK UrhG, § 97 Rn. 86, Rn. 92.
[590] Reber in BeckOK UrhG, § 97 Rn. 93.
[591] BGHZ 148, 13, 17 = BGH GRUR 2001, 1038, 1039 m.w.N.

Gebühr auf Dritte erstreckt, müssen Prüfpflichten verletzt werden, deren Umfang sich danach bestimmt, ob und inwieweit dem Störer nach den Umständen eine Prüfung zuzumuten ist.[592]

Die Rechtsprechung geht regelmäßig von einer Verantwortlichkeit des Host-Providers als Störer aus.[593]

Demnach hat der Host-Provider, nachdem er auf eine konkrete Rechtsverletzung hingewiesen wurde, diese unverzüglich zu entfernen bzw. zu sperren und muss ab diesem Zeitpunkt auch Vorsorge treffen, dass es möglichst nicht zu weiteren derartigen Rechtsverletzungen kommt.[594]

Allerdings kann in der Verletzungshandlung des Nutzers, die Gegenstand des Hinweises war und damit eine Kenntnis des Host-Providers begründet, noch keine Verletzungshandlung gesehen werden, die eine Wiederholungsgefahr im Sinne eines Unterlassungsanspruchs begründet.[595] Für die Annahme einer Wiederholungsgefahr ist eine vollendete Verletzung nach Begründung der Prüfungspflicht im Rahmen der Störerhaftung notwendig.[596]

Etwas anderes kann nach der Rechtsprechung des BGH allerdings für solche Host-Provider gelten, die aktiv Rechtsverletzungen ihrer Nutzer fördern.[597] Sofern das Geschäftsmodell des Host-Providers von vornherein auf Rechtsverletzungen durch die Nutzer angelegt ist oder der Host-Provider durch eigene Maßnahmen die Gefahr einer entsprechenden rechtwidrigen Nutzung fördert, hat er diese Gefahr auszuräumen.[598] Dies bedeutet, dass ihn die Prüfpflichten der Störerhaftung bereits vor Erlangung der Kenntnis einer konkreten Rechtsverletzung treffen können und er im Rahmen

[592] BGH GRUR 2001, 1038, 1039.
[593] So bspw. BGH MMR 2004, 668; BGH MMR 2007, 507; BGH GRUR 2011, 1038; BGH MMR 2013, 185.
[594] BGH GRUR 2011, 1038, 1040.
[595] BGH GRUR 2011, 1038, 1042.
[596] BGH GRUR 2011, 1038, 1042.
[597] BGH MMR 2013, 185, 186; BGH GRUR 2011, 617, 620.
[598] BGH GRUR 2011, 617, 620.

dieser Prüfpflichten verpflichtet ist, die Gefahr zunächst auszuräumen.[599]

aa) Spannungsverhältnis § 10 TMG und Störerhaftung

Ausgangspunkt für die Problematik auf europäischer Ebene ist das Spannungsverhältnis zwischen den Privilegien in §§ 12-14 ECRL und den gerichtlichen Anordnungen nach Art. 8 Abs. 3 InfoSoc-RL für Verletzungen des Urheberrechts bzw. Art. 11 S. 3 Durchsetzungs-RL für Verletzungen anderer geistiger und gewerblicher Schutzrechte.

Artikel 11 S. 3 der Durchsetzungs-RL bzw. für den Bereich des Urheberrechts Art. 8 Abs. 3 InfoSoc-RL behandelt die Verpflichtung der Mitgliedstaaten gerichtliche Anordnungen gegen Mittelspersonen beantragen zu können, deren Dienste von einem Dritten zwecks Verletzung eines Rechts des geistigen Eigentums in Anspruch genommen werden.

Das deutsche Pendant hierzu stellen die §§ 8-10 TMG sowie die Störerhaftung dar. Der deutsche Gesetzgeber hat darauf verzichtet Art. 8 Abs. 3 InfoSoc-RL bzw. Art. 11 S. 3 Durchsetzungs-RL durch eine neue explizite Regelung umzusetzen, da er der Auffassung war, dass bereits nach geltendem Recht Anordnungen gegen Vermittler beantragt werden können.[600] Nach § 97 Abs. 1 S. 1 UrhG und ständiger Rechtsprechung könne der Provider als Störer auf Unterlassung in Anspruch genommen werden, wobei hier die Regelungen des §§ 8 ff. TDG a.F. zu beachten seien.[601] Dass die Bestimmungen hinsichtlich der Anordnungen gegen Vermittler nicht das Haftungsregime der E-Commerce-RL berühren, stellen auch der Erwägungsgrund 16 der InfoSoc-RL sowie Art. 2 Abs. 3 Durchsetzungs-RL klar.

Wie bereits ausgeführt, ging die Rechtsprechung zumindest früher davon aus, dass die Privilegierung des § 10 TMG keine Anwendung auf Unterlassungsansprüche findet. In seiner neueren Rechtsprechung prüft der BGH den § 10 TMG allerdings auch im

[599] BGH MMR 2013, 185, 186.
[600] BT-Drucks. 15/38, S. 39; BT-Drucks. 16/5048, S. 32.
[601] BT-Drucks. 15/38, S. 39 f.

Rahmen der Störerhaftung. In der Folge sieht er i.d.R. keine Verantwortlichkeit des Host-Providers, sofern dieser keine Kenntnis gem. § 10 S. 1 Nr. 1 TMG hat bzw. unverzüglich gem. § 10 S. 1 Nr. 2 TMG tätig geworden ist, um die rechtsverletzende Information zu entfernen bzw. zu sperren.[602]

Im Anschluss an die Kenntnis und die damit einhergehende Entfernung bzw. Sperrung ist der Host-Provider entgegen der Bestimmung des § 10 TMG aber nicht von einer Verantwortlichkeit privilegiert, sondern ihn treffen Prüfpflichten, welchen er nachkommen muss, um einer Haftung als Störer zu entgehen.[603]

Der BGH begründet dies mit Art. 11 S. 3 Durchsetzungs-RL, welcher nach dem EuGH dahingehend auszulegen ist, dass die nationalen Gerichte dem Host-Provider Maßnahmen auferlegen können, die nicht nur zur Beendigung der auf seiner Plattform von Nutzern begangene Rechtsverletzungen, sondern auch wirksam zur Vorbeugung gegen erneute Verletzungen beitragen.[604] Deshalb sei der Host-Provider verantwortlich, sobald er Kenntnis hat und ab diesem Zeitpunkt treffe ihn die durch einen Unterlassungsanspruch durchsetzbare Verpflichtung, zukünftig derartige Verletzungen zu verhindern.[605]

Bedenklich ist aber zum einen die automatisch eintretende Prüfungsverpflichtung des Host-Providers als auch die Reichweite der Prüfpflichten im Hinblick auf § 10 TMG i.V.m. § 7 Abs. 2 S. 1 TMG.

bb) Zumutbare Prüfpflichten nach Kenntnis

Nach höchstrichterlicher Rechtsprechung treffen den Host-Provider nach Kenntnis über eine Urheberrechtsverletzung automatisch Prüfpflichten, um einer Inanspruchnahme als Störer zu entgehen.[606]

Bei einem besonders gefahrgeneigten Dienst sollen den Host-

[602] Etwas anderes könnte lediglich für sog. gefahrgeneigte Dienste gelten. Dies hat der BGH bislang aber offen gelassen.
[603] BGH GRUR 2011, 1038, 1039.
[604] BGH GRUR 2011, 1038, 1040.
[605] BGH GRUR 2011, 1038, 1040.
[606] Vgl. BGH GRUR 2011, 1038, 1040 m.w.N.

Provider zudem bereits vor Kenntnis entsprechende Prüfungspflichten treffen.[607]

Ob und inwieweit dem Störer eine Prüfung zuzumuten ist, richtet sich nach den jeweiligen Umständen des Einzelfalls unter Berücksichtigung der spezifischen Funktion und Aufgabenstellung des Host-Providers, dem Gewicht der angezeigten Rechtsverletzung sowie der Eigenverantwortung des unmittelbaren Verletzers.[608]

Als Bewertungskriterium ist u.a. zu berücksichtigen, ob der Host-Provider an der Rechtsverletzung, bspw. durch Provision, profitiert und ob die Rechtsverletzung aufgrund einer unklaren Rechtslage erst nach eingehender rechtlicher oder tatsächlicher Prüfung festgestellt werden kann oder aber für den Host-Provider unschwer zu erkennen ist.[609]

Im Laufe der letzten Jahre hatte der BGH des Öfteren die Gelegenheit, sich mit der Frage der Zumutbarkeit von Prüfpflichten des Host-Providers auseinanderzusetzen.

Als grundsätzlich zumutbar sieht der BGH den Einsatz von Filtersoftware, die durch Eingabe entsprechender Suchbegriffe Verdachtsfälle aufdeckt sowie die ggf. anschließend notwendige manuelle Nachprüfung.[610] Durch den Einsatz sollen allerdings nicht nur die neu auf den Server des Host-Providers geladenen Dateien ausgefiltert werden, sondern auch die bereits dort gespeicherten Daten überprüft werden.[611]

Die wohl umfangreichsten Prüfpflichten wurden bislang den File-Hosting-Diensten auferlegt.[612] Während der I. Zivilsenat in seinem „Alone in the Dark"-Urteil noch die manuelle Kontrolle jedenfalls einer einstelligen Zahl von Linksammlungen als für den Host-Provider zumutbar ansah[613], sah er im „Rapidshare"-Urteil keine Notwendigkeit der Begrenzung der zu überprüfenden

[607] BGH MMR 2013, 185, 186.
[608] BGH GRUR 2011, 1038, 1039.
[609] BGH MMR 2013, 185, 187; BGH GRUR 2011, 1038, 1039 f.
[610] BGH MMR 2007, 507, 511; BGH MMR 2004, 668, 672.
[611] BGH MMR 2013, 185, 187.
[612] BGH GRUR 2013, 1030, 1034; BGH MMR 2013, 185, 187.
[613] BGH MMR 2013, 185, 188.

Linksammlungen, da es sich bei dem konkreten Geschäftsmodell des Host-Providers um ein solches handele, dass Urheberrechtsverletzungen in erheblichem Umfang Vorschub leiste[614].

Generell stellt der Senat im letztgenannten Urteil fest, dass, sofern das Geschäftsmodell des Host-Providers strukturell die Gefahr massenhafter Urheberrechtsverletzungen berge, diesen erheblich gesteigerte Prüfpflichten träfen.[615] Diese Gefahr sah er im zu entscheidenden Fall darin, dass der Host-Provider seine Nutzer dazu ermutigt hätte, die hochgeladenen Dateien möglichst breit und flächendeckend zu verteilen sowie die Vergabe von Premium-Punkten an die Häufigkeit des Herunterladens der Dateien gekoppelt hat.[616] Zudem wurde dem Nutzer ein vollständig anonymes Handeln ermöglicht.[617]

cc) Umfang der Prüfpflicht- Kerngleichheit

Nach der ständigen Rechtsprechung des BGH trifft den Host-Provider nach Kenntnis grundsätzlich die Pflicht Vorsorge zu treffen, dass es nicht zu weiteren gleichartigen Rechtsverletzungen kommt.[618] Fraglich ist insbesondere was genau unter dem Begriff der „gleichartigen“ oder „derartigen“ Rechtsverletzungen fällt.

Der BGH hat für den Bereich der Urheberrechtsverletzung ausgeführt, dass hierunter das konkret benannte urheberrechtliche Werk fällt, das allerdings auch durch andere Nutzer zugänglich gemacht werden kann.[619]

Wie der Umfang bei einer Prüfpflicht bereits vor Kenntnis bestimmt werden soll, ist unklar. Da der BGH ausführt, der Host-Provider eines besonders gefahrgeneigten Dienstes sei verpflichtet, die Gefahr auszuräumen, könnte hierauf geschlossen werden, dass sich die Prüfpflicht auf den gesamten Inhalt des Dienstes bezieht.

---

[614] BGH GRUR 2013, 1030, 1034.
[615] BGH GRUR 2013, 1030, 1030.
[616] BGH GRUR 2013, 1030, 1031.
[617] BGH GRUR 2013, 1030, 1031.
[618] BGH MMR 2013, 185, 187; BGH GRUR 2011, 1038, 1040; BGH MMR 2004, 668, 672.
[619] BGH GRUR 2013, 1030; BGH MMR 2013, 185, 187.

Denn nur so könnte der Host-Provider theoretisch sicherstellen, dass die Gefahr von Rechtsverletzungen ausgeräumt ist.

dd) Bewertung Prüfpflichten

Fraglich ist, wie die vom BGH angeführten zumutbaren Prüfpflichten, auch hinsichtlich kerngleicher Rechtsverstöße, mit dem in § 7 Abs. 2 S. 1 TMG enthaltenen allgemeinen Überwachungs- und Nachforschungsgebot vereinbar sind.

Der EuGH hat in der „SABAM/Netlog"-Entscheidung die Verpflichtung eines Host-Providers zur Einrichtung eines Filtersystems, das die von seinen Nutzern auf seinem Server gespeicherten Informationen unterschiedslos von allen Nutzern, präventiv und zeitlich unbegrenzt filtert, ausdrücklich für unzulässig erklärt.[620]

Der Gerichtshof führte hier aus, dass eine entsprechende gerichtliche Anordnung nach Art. 8 Abs. 3 InfoSoc-RL und Art. 11 S. 3 Durchsetzungs-RL eine aktive Beobachtung der von den Nutzern beim Host-Provider gespeicherten Dateien erfordere und sich auf fast alle Informationen sowie sämtliche Nutzer beziehe.[621] Der Host-Provider wäre folglich dazu verpflichtet eine aktive Überwachung vorzunehmen, um jeder künftigen Verletzung von Urheberrechten vorzubeugen, was den Mitgliedsstaaten gem. Art. 15 Abs. 1 ECRL verboten sei.[622]

Zudem müssten die widerstreitenden Grundrechte gegeneinander abgewogen werden, genauer gesagt der Schutz des Rechts am geistigen Eigentum, der Schutz der unternehmerischen Freiheit sowie der Schutz personenbezogener Daten sowie der Informationsfreiheit, um so ein angemessenes Gleichgewicht sicherzustellen.[623] Eine umfangreiche Filterverpflichtung wäre als qualifizierte Beeinträchtigung der unternehmerischen Freiheit zu

[620] EuGH GRUR 2012, 382.
[621] EuGH GRUR 2012, 382, 383.
[622] EuGH GRUR 2012, 382, 383.
[623] EuGH GRUR 2012, 382, 384.

werten, welche zudem die Grundrechte der Nutzer beeinträchtige und ein angemessenes Gleichgewicht nicht gewährleiste.[624]

Die Verpflichtung des Host-Providers im Rahmen der Störerhaftung zur Verhinderung erneuter gleichartiger Rechtsverletzungen würde im Ergebnis auf den Einsatz eines präventiven, zeitlich unbegrenzten und unterschiedslos auf alle Nutzer anwendbaren Filtersystems hinauslaufen.[625]

Um kerngleiche Urheberrechtsverletzungen aufzudecken, das heißt auch solche von anderen Nutzern und nicht lediglich solche des originären Verletzers, müssten sämtliche Inhalte das Filtersystem passieren sowie ggf. manuell nachgeprüft werden.

Diese Überwachungsverpflichtung, alle Inhalte sämtlicher Nutzer auf unbestimmte Zeit, nur um den Upload einer bekannt gewordenen Rechtsverletzung zu verhindern, kann nicht als Überwachung in einem spezifischen Fall klassifiziert werden, da diese den Host-Provider faktisch zu einer allumfassenden Überwachung verpflichtet, welche nach § 7 Abs. 2 S. 1 TMG gerade nicht verlangt werden darf.[626]

Die Argumentation, dass es sich hierbei nicht um allgemeine Überwachungspflichten handele, sondern lediglich um solche im spezifischen Fall, ist daher abzulehnen.[627]

Zudem würde eine solche allgemeine Prüfpflicht auch nicht die von ihr betroffenen Grundrechte in angemessener Weise berücksichtigen.

Auch der EuGH geht in seiner „L'Oréal"-Entscheidung von einem anderen Verständnis der deutschen Kerntheorie aus, indem er ausführt, dass der Host-Provider durch eine gerichtliche Anordnung nicht nur Maßnahmen zur Beendigung einer Rechtsverletzung, sondern auch zur Vorbeugung erneuter derartiger Rechtsverletzungen auferlegt werden können, sofern diese wirksam, verhältnismäßig und abschreckend seien sowie

[624] EuGH GRUR 2012, 382, 384.
[625] So auch Rauer, GRUR-Prax 2013, 93, 93.
[626] Hoeren in Festschrift für Ulricht Eisenhardt, S. 243, 251; Hoeren/Yankova, IIC 2012, 501, 529.
[627] So auch Hoeren in Festschrift für Ulrich Eisenhardt, S. 243, 251.

keine Schranken für den rechtmäßigen Handel errichteten.[628] Denkbar seien daher der Ausschluss des Verletzers oder Maßnahmen zur Erleichterung der Identifizierung seiner Nutzer.[629]

Der Gerichtshof weist nochmals darauf hin, dass die von ihm dargestellten Maßnahmen in Gestalt einer Anordnung i.S.v. Art. 11 S. 3 Durchsetzungs-RL aufzuerlegen sind.[630]

Auch das urheberrechtliche Pendant in Art. 8 Abs. 3 InfoSoc-RL spricht von einer gerichtlichen Anordnung.

Die Prüfpflichten im Rahmen der Störerhaftung treffen den Host-Provider jedoch automatisch nach Kenntnis einer bestimmten Rechtsverletzung und nicht erst im Rahmen einer gerichtlichen Anordnung. Zwar sind die Bedingungen und Modalitäten einer solchen Anordnung nach nationalem Recht zu regeln.[631] Dies ändert aber nichts an dem Erfordernis einer gerichtlichen Anordnung. Auch Art. 14 Abs. 3 ECRL erfordert den Erlass einer Anordnung durch ein Gericht oder eine Verwaltungsbehörde.

Nach Art. 14 Abs. 3 2. Alt. ECRL können die Mitgliedstaaten lediglich Verfahren für die Entfernung einer Information oder die Sperrung des Zugangs zu ihr festlegen. Dies ist dahingehend auszulegen, dass es den Mitgliedstaaten unbenommen bleibt eigene *Notice and Takedown*-Regelungen[632], angelehnt an das US-amerikanische Vorbild, festzulegen.[633] Dies ergibt sich auch aus den 46. Erwägungsgrund der ECRL, wonach die Mitgliedstaaten spezifische Anforderungen vorschreiben können, die vor der Entfernung von Informationen oder der Sperrung des Zugangs unverzüglich zu erfüllen sind.[634] Hierauf gestützt werden kann hingegen nicht die Schaffung zusätzlicher Voraussetzungen zur Privilegierung nach § 10 TMG. Die Voraussetzungen des § 10

---

[628] EuGH MMR 2011, 596, 605.
[629] EuGH MMR 2011, 596, 604 f.
[630] EuGH MMR 2011, 596, 605.
[631] Erwägungsgrund 59 der InfoSoc-RL.
[632] Zum US-amerikanischen Notice and Takedown-Verfahren siehe S. 296 .
[633] So auch Holznagel, S. 84; Siehe hierzu auch http://ec.europa.eu/internal_market/e-commerce/notice-and-action/index_en.htm, zuletzt besucht am 23.04.2016.
[634] Hierunter kann die Erfüllung formeller Voraussetzungen fallen, bspw. durch Versendung einer Mitteilung mit spezifischem Inhalt.

TMG für eine Haftungsfreistellung des Host-Providers sind insoweit als abschließend anzusehen.[635]

Noch kritischer sind die Ausführungen des BGH hinsichtlich gefahrgeneigter Dienste zu sehen. So soll den Host-Provider in diesem Fall bereits vor Kenntnis einer spezifischen Rechtsverletzung eine Prüfpflicht treffen können, die ihn dazu verpflichtet, die Gefahr, die von seinem Dienst ausgeht, zunächst auszuräumen. Während der I. Zivilsenat in seinem „Alone in the Dark"-Urteil eine entsprechende Pflicht sowohl bei einem Geschäftsmodell, welches von vornherein auf Rechtsverletzungen seiner Nutzer angelegt ist, als auch bei einer Förderung der rechtsverletzenden Nutzung durch eigene Maßnahmen als möglich erachtet[636], scheint er in seinem „File-Hosting-Dienst"-Urteil davon auszugehen, dass eine solche Pflicht lediglich bei Diensten, welche von vornherein auf Rechtsverletzungen angelegt sind, möglich ist.[637] Verwunderlich hinsichtlich der abweichenden Bewertung der Prüfpflichten im Rahmen dieser beiden Urteile ist auch, dass es sich um den identischen Dienst handelte und der erkennende Senat für die unterschiedliche Bewertung lediglich auf die in dem „Alone in the Dark"-Urteil getroffenen tatrichterlichen Feststellungen verweist.[638] Welche genau das sein sollen, ist unklar. Folge dieser auf unbekannten Tatsachen beruhenden und scheinbar willkürlichen Rechtsprechung des Senats ist die Schaffung erheblicher Unsicherheiten zulasten der Host-Provider.[639]

So weist auch *Völzmann-Stickelbrock*, die grundsätzlich eine Verschärfung der Prüfpflichten für gefahrgeneigte Host-Provider begrüßt, darauf hin, dass mit der Annahme einer besonderen

---

[635] So auch Szpunar, Schlussanträge vom 16.03.2016, Rn. 97 hinsichtlich der Voraussetzungen für die Privilegierung des Access-Providers.
[636] BGH MMR 2013, 185, 186.
[637] Siehe MMR 2013, 185, 186: *„[...] ist es ihr [...] nicht zuzumuten, jede von Nutzern auf ihren Servern hochgeladene Datei auf rechtsverletzende Inhalte zu untersuchen. Dies würde ihr Geschäftsmodell gefährden, das nicht von vornherein auf Rechtsverletzungen durch die Nutzer angelegt ist [...]."*
[638] GRUR 2013, 1030, 1032.
[639] So im Ergebnis auch Hoeren, NJW 2013, 3250, 3251.

Gefahrgeneigtheit vorsichtig umzugehen sei, da sonst von dem grundsätzlichen Privileg nicht mehr viel übrig bliebe.[640]

Die Verpflichtung einer Prüfungspflicht vor Kenntnis einer konkreten Rechtsverletzung kommt zudem einer generellen präventiven Überwachungspflicht gleich, weshalb hier bereits ein Verstoß gegen § 7 Abs. 2 S. 1 TMG vorliegt. Zudem würde ein solcher Host-Provider durch die vor Kenntnis auferlegten Pflichten schon nicht der Privilegierung des § 10 TMG unterliegen, da er bereits vor Kenntnis einer Rechtsverletzung tätig werden müsste, um einer Haftung zu entgehen.

ee) Zwischenergebnis

Das vom BGH konstruierte Konzept der Störerhaftung des Host-Providers nach Kenntnis einer Rechtsverletzung und die damit einhergehenden Prüfpflichten verstoßen sowohl gegen § 7 Abs. 2 S. 1 TMG als auch § 10 TMG. Dies gilt erst Recht für die vom BGH aufgestellten Grundsätze hinsichtlich eines gefahrgeneigten Dienstes. Eine Rechtfertigung für die Auferlegung solcher Prüfpflichten könnte nach den vom EuGH aufgestellten Grundsätzen lediglich eine aktive Rolle sein, welche dem Host-Provider eine Kenntnis oder Kontrolle der spezifischen Inhalte verschafft.

Durch die vom BGH dem Host-Provider auferlegten Prüfpflichten im Rahmen der Störerhaftung wird nicht nur faktisch eine generelle Überwachungspflicht begründet, sondern auch eine zusätzliche Voraussetzung geschaffen, welcher der Host-Provider erfüllen muss, um einer Verantwortlichkeit zu entgehen.

ff) Rechtsfolgen

Haftet der Host-Provider als Störer, so steht dem Berechtigten regelmäßig ein Beseitigungs- und Unterlassungsanspruch zu. Fraglich ist, inwieweit auch ein sekundärer Schadensersatzanspruch gegenüber dem Host-Provider geltend gemacht werden kann, wenn dieser nach Kenntnis einer

[640] Völzmann-Stickelbrock, LMK 2013, 352737.

Rechtsverletzung das rechtsverletzende Material nicht entfernt oder er seine Prüfpflichten verletzt.

(1) Beseitigungs- und Unterlassungsanspruch, § 97 Abs. 1 UrhG

Die Haftung als Störer begründet einen Beseitigungs- und Unterlassungsanspruch des Urheberrechtsinhabers.

Dieser setzt jedoch eine Wiederholungsgefahr voraus.

Nach der Rechtsprechung des BGH fehlt es bei derjenigen Verletzungshandlung, die dem Host-Provider Kenntnis hinsichtlich einer Rechtverletzung vermittelt und damit eine Prüfpflicht begründet i.d.R. an einer solchen Wiederholungsgefahr.[641] Hierfür ist eine vollendete Verletzung nach Begründung der Prüfpflichten im Rahmen der Störerhaftung notwendig.[642] Etwas anderes soll allerdings für gefahrgeneigte Dienste gelten.[643]

Kommt es folglich nach Kenntnis über eine Rechtsverletzung zu einer erneuten derartigen Rechtsverletzung auf der Plattform des Host-Providers, wird hierdurch die für einen Unterlassungsanspruch notwendige Wiederholungsgefahr erst begründet. Allerdings hat das Gericht im Rahmen der Auferlegung einer Unterlassungsverpflichtung zu prüfen, ob der Host-Provider überhaupt gegen die Prüfpflichten verstoßen hat und er entsprechend als Störer haftet, d.h. ob er zumutbare Maßnahmen zur Verhinderung derartiger Rechtsverletzungen getroffen hat. Die zumutbare Prüfpflicht ist folglich dem Tatbestand zuzuordnen und nicht erst der Rechtsfolgenseite.[644] Denn ohne eine Verletzung zumutbarer Prüfpflichten darf schon keine Verurteilung zur Unterlassung erfolgen. Wird der Host-Provider schließlich aufgrund einer Verletzung seiner zumutbaren Prüfpflichten als Störer auf Unterlassung verurteilt, trifft ihn wiederum im

[641] BGH GRUR 2011, 1038, 1042.
[642] BGH GRUR 2011, 1038, 1042.
[643] BGH MMR 2013, 185, 186.
[644] BGH ZUM 1999, 144, 145; Haedicke, GRUR 1999, 397, 402; Klatt, ZUM 2009, 265, 266; Leistner, GRUR 2006, 801, 804, 813; Spindler, MMR 2007, 511, 512; a.A. Peifer, AfP 1/2014, 18, 20, 23 noch mit Bezug auf die frühere Rechtsprechung des BGH in NJW 1976, 799, 800.

Vollstreckungsverfahren nur eine Verantwortlichkeit für Zuwiderhandlungen gegen seine Unterlassungsverpflichtung, sofern diese Zuwiderhandlung auf einem Verschulden beruht, d.h. falls der Host-Provider ihm zumutbare Prüfpflichten unterlassen hat.[645] Die Verletzung zumutbarer Prüfpflichten wird folglich an zwei Stellen geprüft. Zunächst bei der Frage, ob der Host-Provider überhaupt als Störer auf Unterlassung verpflichtet werden kann und dann im Vollstreckungsverfahren, für den Fall, dass er gegen diese Unterlassungsverpflichtung verstößt.

(2) Schadensersatzanspruch, § 97 Abs. 2 UrhG

Fraglich ist, ob den Störer auch eine Schadensersatzpflicht treffen kann, falls er seine Prüfpflichten verletzt und es folglich zu einer erneuten Rechtsverletzung kommt.

Auch wenn die verschuldensunabhängige Störerhaftung, im Unterschied zur deliktischen Haftung, originär lediglich eine Verpflichtung zur Entfernung und Unterlassung begründet, wird teilweise im Schrifttum davon ausgegangen, dass jedenfalls sofern der Host-Provider nach Kenntnis von einer Rechtsverletzung keine zumutbaren Maßnahmen zur Verhinderung zukünftiger Rechtsverletzungen trifft, so dass es zu einer erneuten Urheberrechtsverletzung kommt, auch eine Schadensersatzverpflichtung (sog. sekundäre Schadens-ersatzpflicht) nicht ausgeschlossen ist.[646] Es geht also nicht um eine Schadensersatzpflicht nach tatsächlicher Kenntnis des Host-Providers von einer Rechtsverletzung, sondern um eine Schadensersatzpflicht die daraus folgt, dass der Host-Provider seinen Prüfpflichten nach Kenntnis einer Rechtsverletzung nicht nachkommt und es deswegen zu einer erneuten Rechtsverletzung kommt, ohne dass der Host-Provider hiervon jedoch Kenntnis hat.

Diese Ansicht ist abzulehnen. Sofern die originäre Tätigkeit des Host-Providers keine Einordnung als Täter/Teilnehmer im Sinne einer willentlichen Mitwirkung an der ursprünglich öffentlichen

[645] BGH MMR 2007, 507, 511.
[646] Ensthaler/Heinemann, GRUR 2012, 433, 439; Klatt, ZUM 2009, 265, 271; Krüger/Apel, MMR 2012, 144, 148.

Zugänglichmachung rechtfertigt, kann auch eine daran anschließende Verletzung seiner Prüfpflichten keine entsprechende Schadensersatzpflicht begründen. Eine entsprechende Schadensersatzspflicht würde auch bereits an § 10 S. 1 Nr. 2 TMG scheitern, da der Host-Provider auch für den Fall der Verletzung seiner Prüfpflichten regelmäßig keine Kenntnis des konkret durch Verletzung seiner Prüfpflichten betroffenen rechtsverletzenden Inhalt hat.

Denkbar wäre allenfalls eine Schadensersatzpflicht für den Fall, dass der Host-Provider rechtswidriges Urheberrechtsmaterial, von dem er positive Kenntnis hat, in vorwerfbarer Weise nicht entfernt. Hierbei muss allerdings beachtet werden, dass diese Haftung nicht bereits aus § 10 S. 1 Nr. 2 TMG gefolgert werden kann, da § 10 TMG keine Verantwortlichkeit des Host-Providers begründet, sondern lediglich die Voraussetzungen seiner Privilegierung festlegt.

Geht man davon aus, dass die Störerhaftung ab dem Zeitpunkt der Kenntnis dem Host-Provider eine Pflicht zur Entfernung auferlegt, so ist denkbar, dass aus der Störerhaftung eine Haftung als Täter erwächst, nachdem der Host-Provider sich in voller Kenntnis der Rechtswidrigkeit des streitgegenständlichen Inhalts weigert, diesen zu entfernen.

Dogmatisch ließe sich dies unter Umständen wie folgt begründen. Hat der Host-Provider Kenntnis von einer konkreten Rechtsverletzung und weigert sich dennoch diese zu entfernen oder zu sperren, verliert er seine privilegierte Position, die ihm § 10 TMG gewährt. Seine Verantwortlichkeit beurteilt sich folglich nach den allgemeinen Gesetzen. Hier wäre eine Anwendbarkeit des Konstruktes des zu eigen Machens fremder Inhalte denkbar. Durch die Weigerung des Host-Providers, den urheberrechtswidrigen Inhalt zu löschen, hätte der Host-Provider diesen auf Grund einer bewussten Entscheidung als Teil seines eigenen Dienstes in sein Leistungsangebot aufgenommen. Der Inhalt wäre ihm folglich als eigener zuzurechnen, für den er als Täter wegen schuldhafter

Verletzung des Urheberrechts auch Schadensersatz i.S.d. § 97 Abs. 2 UrhG zu leisten hätte.

Ob eine solche bewusste Entscheidung allerdings alleine ausreichend ist, um dem Host-Provider die fremden Inhalte als eigene zuzurechnen, ist fraglich.[647] In „marions.kochbuch.de“ hat der I. Zivilsenat jedenfalls eine Gesamtbetrachtung aller relevanten Umstände vorgenommen und sowohl auf die redaktionelle Vorabkontrolle durch den Host-Provider als auch die Erweckung eines zurechenbaren Anscheins, dass er sich mit den fremden Inhalten identifiziere, abgestellt.[648]

c) Ergebnis

Ein Beseitigungs- und Unterlassungsanspruch gegen den Host-Provider als Täter oder Teilnehmer scheidet regelmäßig aus, sofern dieser nicht willentlich an einer Rechtsverletzung mitgewirkt hat bzw. sich die Inhalte Dritter zu eigen gemacht hat. Denkbar ist eine Haftung auf Beseitigung und Unterlassung als Störer. Fragwürdig ist allerdings die durch die Störerhaftung begründete Prüfpflicht des Host-Providers nach Kenntnis von einer Rechtsverletzung sowie eine entsprechende Anwendung der Kerntheorie.

Bejaht man sowohl eine Störerhaftung aufgrund der Verletzung von Prüfpflichten nach Kenntnis des Host-Providers als auch eine Unterlassungsverpflichtung, nicht beschränkt auf die Entfernung bzw. Sperrung der konkreten Rechtsverletzung, würde dies bedeuten, dass die Prüfpflichten als Voraussetzung für die Haftung als Störer zunächst auf Tatbestandsebene bei der Prüfung des Unterlassungsanspruchs angesiedelt werden müssen und anschließend nochmals im Rahmen des Vollstreckungsverfahrens bei der Frage des Verschuldens des Host-Providers.

Im Ergebnis führt dies zu einer erheblichen Rechtsunsicherheit seitens des Host-Providers, was der Zielsetzung der ECRL und des TMG entgegen stehen dürfte.

---

[647] Dafür: Leupold in Leupod/Glossner, Teil 2, Rn. 594; Siebers, Rn. 302.
[648] BGH GRUR 2010, 616, 618 f.

Gleiches gilt für die Begründung einer Prüfpflicht bereits vor Kenntnis einer spezifischen Rechtsverletzung für gefahrgeneigte Dienste. Eine entsprechende Pflicht würde den Host-Provider faktisch zu einer Überwachung seines gesamten Dienstes verpflichten, was im Widerspruch zu § 7 Abs. 2 S. 1 sowie Art. 15 Abs. 1 ECRL stünde. Eine andere Beurteilung wäre im Licht der EuGH-Rechtsprechung lediglich möglich, sofern es sich bei dem gefahrgeneigten Dienst um einen aktiven Host-Provider handelt, der Kenntnis oder Kontrolle des spezifischen Inhaltes erlangt.

2. Strafrechtliche Verantwortlichkeit des Host-Providers

Neben der zivilrechtlichen Verantwortlichkeit kann den Host-Provider auch eine strafrechtliche Verantwortlichkeit treffen. Das Urheberrechtsgesetz enthält in den §§ 106 ff. entsprechende Straf- und Bußgeldvorschriften. Im Rahmen der Tätigkeit des Host-Providers kommen regelmäßig die folgenden Straftatbestände in Betracht.

a) Unerlaubte Verwertung urheberrechtlich geschützter Werke, § 106 UrhG

Nach § 106 UrhG kann derjenige, der in anderen als den gesetzlich zugelassenen Fällen ohne Einwilligung des Berechtigten ein Werk vervielfältigt, verbreitet oder öffentlich wiedergibt, mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft werden.

aa) In anderen als den gesetzlich zugelassenen Fällen

§ 106 UrhG nennt die gesetzlich zugelassenen Fälle als negatives Tatbestandsmerkmal, welches bei Vorliegen bereits den Tatbestand nicht erfüllt und nicht lediglich einen Rechtfertigungsgrund darstellt.[649] Hierzu zählen insbesondere die Schrankenbestimmungen der §§ 44a ff. sowie §§ 69d f. UrhG.[650]

[649] Heinrich in MüKo StGB, § 106 UrhG, Rn. 78.
[650] Heinrich in MüKo StGB, § 106 UrhG, Rn. 78.

bb) Vervielfältigung, Verbreitung oder öffentliche Wiedergabe

Die bei dem Host-Provider maßgebliche Verwertungsform ist regelmäßig die Vervielfältigung i.S.d. § 16 UrhG sowie die öffentliche Zugänglichmachung i.S.d. § 19a UrhG durch Speicherung des Inhalts auf seinem Server.

cc) Vorsatz

Auch wenn die gesetzliche Bestimmung dies nicht ausdrücklich benennt, ist lediglich vorsätzliches Handeln im Rahmen des § 106 UrhG strafbar.[651] Dies ergibt sich aus dem allgemeinen Grundsatz des § 15 StGB, dass nur vorsätzliches Handeln strafbar ist und fahrlässiges Handeln lediglich, sofern dies im Gesetz ausdrücklich mit Strafe bedroht ist. Bedingter Vorsatz ist insofern ausreichend.[652] Hinsichtlich des Host-Providers dürfte Vorsatz i.d.R. fehlen. Selbst sofern sich der Host-Provider Inhalte zu eigen gemacht hat, ist fraglich, ob er mindestens den Erfolg für möglich gehalten hat und diesen billigend in Kauf genommen hat. Möglich wäre ein vorsätzliches Handeln als Teilnehmer. Wie bereits erläutert, bedarf es hierfür eines doppelten Vorsatzes. Ob ein solcher vorliegt, ist anhand der spezifischen Umstände des Einzelfalls zu bestimmen. Insbesondere bei

dd) Keine Einwilligung

Der Host-Provider kann sich lediglich strafbar machen, sofern keine Einwilligung des Berechtigten vorliegt. Die Einordnung der Einwilligung im Rahmen des § 106 StGB ist strittig. Sie wird entweder lediglich der Rechtswidrigkeitsebene zugeordnet oder ihr wird eine Doppelfunktion in dem Sinne zugesprochen, dass auf Tatbestandsebene die Nichtberechtigung zu prüfen ist, während im Rahmen der Rechtswidrigkeit die allgemeine strafrechtliche Einwilligung zu prüfen ist.[653]

---

[651] Heinrich in MüKo StGB, § 106 UrhG, Rn. 119.
[652] Heinrich in MüKo StGB, § 106 UrhG, Rn. 119.
[653] Für eine Zuordnung auf Rechtswidrigkeitsebene: Dreier in Dreier/Schulze, § 106 Rn. 8; Heinrich in MüKo StGB, § 106 UrhG, Rn. 115; für eine Doppelfunktion: Sternberg-Lieben in BeckOK UrhG, § 106 Rn. 33; Hildebrandt/Reinbacher in Wandtke/Bullinger § 106 Rn. 24.

b) Gewerbsmäßige unerlaubte Handlung, § 108a UrhG

Für den Fall, dass der Host-Provider gem. § 106 UrhG strafrechtlich verantwortlich ist, kann er im Falle einer gewerbsmäßigen Verwertung zu einer Freiheitsstrafe bis zu fünf Jahren verurteilt werden.

§ 108a UrhG stellt einen Qualifikationstatbestand des § 106 UrhG dar.[654]

Der Begriff der Gewerbsmäßigkeit ist im strafrechtlichen Sinne zu verstehen und liegt vor, wenn der Host-Provider sich aus wiederholter Tatbegehung eine nicht nur vorübergehende Einnahmequelle von einigem Umfang verschaffen will.[655] Unerheblich ist, ob er einen Gewerbebetrieb betreibt oder nicht.[656] Von Bedeutung ist vielmehr eine gewisse Dauerhaftigkeit der Tätigkeit, wofür bereits die erste Tat ausreichen kann, sofern aus ihr geschlossen werden kann, dass der Host-Provider eine entsprechende Absicht hat.[657]

c) Ergebnis

Eine strafrechtliche Verantwortlichkeit des neutralen Host-Providers ist im Regelfall zu verneinen, da es hierfür am erforderlichen Vorsatz fehlen dürfte. Im Einzelfall ist jedoch insbesondere eine Einordnung als Teilnehmer denkbar, sofern der Host-Provider sowohl mit Vorsatz hinsichtlich der Haupttat des Dritten als auch mit Vorsatz seiner eigenen Tathandlung handelt.

Er kann dann § 106 UrhG mit bis zu drei Jahren bzw. bei gewerbsmäßigem Handeln gem. § 108a UrhG bis zu fünf Jahren Freiheitsstrafe oder Geldstrafe verurteilt werden.

Es handelt sich gem. § 109 UrhG um ein relatives Antragsdelikt, d.h. das Tätigwerden der Staatsanwaltschaft setzt einen entsprechenden Strafantrag des Verletzten voraus.

---

[654] Hildebrandt/Rheinbacher in Wandtke/Bullinger, § 108a Rn. 1.
[655] Dreier in Dreier/Schulze, § 108a Rn. 5.
[656] Dreier in Dreier/Schulze, § 108a Rn. 5.
[657] Dreier in Dreier/Schulze, § 108a Rn. 6.

Eine strafrechtliche Verantwortlichkeit des reinen Störers ist ausgeschlossen.[658] Hier fehlt es bereits an einem vorsätzlichen Handeln. Auch eine Unterlassungsstrafbarkeit für den Fall, dass der Störer seinen Prüfpflichten nicht nachkommt, ist aufgrund der fehlenden Garantenstellung auszuschließen.[659]

3. Zivilrechtliche Verantwortlichkeit des Cache-Providers

Eine Haftung des Cache-Providers ist nach den allgemeinen Haftungsgrundsätzen entweder als Täter/Teilnehmer oder Störer einer Urheberrechtsverletzung denkbar.

a) Täter/Teilnehmer

Der Cache-Provider betreibt ein technisches System, welches Inhalte automatisch zur schnelleren Zugangsvermittlung zwischenspeichert. Er hat keinen Einfluss darauf, welche Dateien auf seinen Servern gespeichert werden.[660]

Eine Klassifizierung als Täter kommt somit i.d.R. nicht in Betracht. Auch eine Verantwortlichkeit als Anstifter oder Gehilfe wird regelmäßig nicht gegeben sein.[661] Denkbar wäre lediglich eine Haftung als Anstifter in Fällen, in denen der Cache-Provider derart auf den Willen eines Dritten einwirkt, dass er bei diesem einen Tatentschluss hervorruft. Im Falle des Usenets, steht der Anbieter eines Newsservers regelmäßig nur mit den Nutzern seines eigenen Newsservers in einer vertraglichen Beziehung. Sofern er diesen Speicherplatz auf seinen Newsservern im Rahmen des Usenets zur Verfügung stellt, fungiert er für diese als Host-Provider. Eine Tätigkeit als Cache-Provider ist lediglich in den Fällen gegeben, in denen er Inhalte, die sich auf einem anderen Newsserver befinden, auf Anfrage seiner Nutzer übermittelt und in diesem

[658] So auch Dreier in Dreier/Schulze, § 106 Rn. 6.
[659] Siehe hierzu auch Hildebrandt/Reinbacher in Wandtke/Bullinger, § 106 Rn. 45 sowie Kaiser in Erbs/Kohlhaas, § 106 UrhG, Rn. 39 hinsichtlich des Verstoßes gegen eine Löschungspflicht im Rahmen der §§ 45, 47 Abs. 2 S. 2, § 55 Abs. 1 S. 2, § 56 Abs. 2 UrhG, welche keine Unterlassungsstrafbarkeit begründen soll; a.A. Dreier in Dreier/Schulze, § 106 Rn. 6.
[660] LG München I, MMR 2007, 453, 454.
[661] Ohne weitere Begründung ablehnend auch LG München I, MMR 2007, 453, 454.

Zusammenhang zwischenspeichert.[662] Dabei ist eine Anstiftung Dritter unwahrscheinlich. Der Cache-Provider müsste entweder den Nutzer eines anderen Newsserver-Anbieters dazu anstiften, urheberrechtswidriges Material auf dem Newsserver dieses Dritten zur Verfügung zu stellen oder seine Nutzer dazu anstiften, entsprechend urheberrechtsverletzendes Material herunterzuladen. Es ist bereits fraglich, ob eine solche Anstiftung überhaupt einen positiven Effekt auf das Geschäftsmodell des Cache-Providers hätte. Dies wäre nur der Fall, wenn die Tatsache, dass Dritte auf anderen Newsservern urheberrechtsverletzende Inhalte einstellen, seine Nutzer dazu veranlassen würde, seinen Newsserver zu nutzen und er dadurch neue Kunden gewinnt. Daher ist zu bezweifeln, dass der Cache-Provider als Anstifter tätig wird.
Aus diesem Grund ist auch eine Gehilfenhandlung des Cache-Providers kaum vorstellbar.

b) Störer

Der Cache-Provider könnte jedoch als Störer haften. Der für die Störerhaftung erforderliche adäquat-kausale Beitrag könnte in diesem Fall im Betrieb seines Dienstes liegen, welcher durch die Übermittlung und Zwischenspeicherung von urheberrechtsverletzenden Inhalten zur Urheberrechtsverletzung beiträgt. Zusätzlich müsste der Cache-Provider zumutbare Prüfpflichten verletzt haben.
Die bisher zu dem Cache-Provider ergangene unterinstanzliche Rechtsprechung geht davon aus, dass die Privilegien des TMG auf Unterlassungsansprüche keine Anwendung finden.
Dies haben, ohne weitere Begründung, sowohl das OLG Düsseldorf als auch das LG München I so beurteilt.[663]
Beide sind daher der Auffassung, dass der Cache-Provider, nachdem er Kenntnis von einer bestimmten Urheberrechtsverletzung erlangt hat, grundsätzlich als Störer haftet,

[662] So auch OLG Düsseldorf, MMR 2008, 254, 255.
[663] OLG Düsseldorf, MMR 2008, 254, 255; LG München I, MMR 2007, 453, 455.

sofern er zumutbare Prüfpflichten verletzt hat.[664] Fraglich ist allerdings zum einen, ob die Rechtsprechung zum Host-Provider ohne weiteres auf den Cache-Provider übertragbar ist und zum anderen, ob sich diese Rechtsprechung nach dem geänderten Kurs des BGH, durch den er die Privilegien des Host-Providers grundsätzlich auch auf Unterlassungsansprüche anwendet, überhaupt noch aufrecht erhalten lässt.

aa) Spannungsverhältnis § 9 TMG und Störerhaftung

Problematisch an der Nicht-Anwendung der Privilegien auf die Störerhaftung ist die dem Cache-Provider auferlegte Prüfungspflicht nach Kenntnis über eine Rechtsverletzung. Während § 9 S. 1 Nr. 5 TMG den Cache-Provider ausdrücklich von einer Haftung freistellt, sofern er nach Kenntnis darüber, dass eine Rechtsverletzung auf seinem System gespeichert ist und dass diese am ursprünglichen Ausgangsort entfernt bzw. gesperrt wurde, diese auch entsprechend entfernt, begründet die Störerhaftung eine potentielle weitere Verpflichtung des Cache-Providers, selbst nachdem er den beanstandeten Inhalt entfernt hat. Ihn würden Prüfpflichten zur Verhinderung weiterer Rechtsverletzungen treffen.

Dies würde entsprechend eine zusätzliche Voraussetzung darstellen, welche der Cache-Provider erfüllen muss, um einer Haftung zu entgehen. Die Prüfpflicht würde zudem Inhalte betreffen, welche noch auf der Ursprungsseite abrufbar sind.

bb) Zumutbare Prüfungspflichten nach Kenntnis - bisherige Rechtsprechung

Sowohl das OLG Düsseldorf als auch das LG München I haben ausgeführt, dass den Cache-Provider zumutbare Prüfungspflichten treffen, nachdem er über eine Rechtsverletzung unterrichtet wurde. Beide Fälle behandelten einen Usenet-Betreiber, der seinen Nutzern Zugang zum Usenet vermittelte. Eine Verletzung

[664] OLG Düsseldorf, MMR 2008, 254, 255; LG München I, MMR 2007, 453, 455.

zumutbarer Prüfpflichten wurde letzten Endes in beiden Fällen verneint.

Zur Begründung führte das OLG Düsseldorf aus, dass dem Cache-Provider wesentlich geringere Möglichkeiten zur Verfügung stehen würden, eine Rechtsverletzung abzustellen als bspw. dem Host-Provider.[665] Der Cache-Provider sei nicht dazu in der Lage, das Usenet ständig daraufhin zu überprüfen, ob der beanstandete Inhalt erneut erscheint und daraufhin eine Verbreitung zu unterbinden.[666] Aufgrund des enormen Datenvolumens, der Textkodierung, und der Tatsache, dass er keinen Einfluss auf das Einstellen und Verbreiten von Inhalten im Usenet hat, sei dem Cache-Provider nicht zuzumuten, sämtliches urheberrechtlich geschützte Material von legalen Inhalten zu unterscheiden und den Zugang hierzu zu sperren.[667] Der Cache-Provider könne zudem grundsätzlich nur diejenigen Inhalte löschen, die auf seinem eigenen Server zwischengespeichert sind.[668] Solange der Inhalt aber noch im Usenet verfügbar sei, werde er auf Anforderung eines Nutzers immer wieder auf den Server des Cache-Providers übertragen.[669] Hinzu käme, dass es mit dem Konzept der sog. Cancel-Messages auch Dritten möglich sei, durch das Senden einer speziellen Nachricht einen bestimmten Inhalt weltweit auf allen Newsservern zu löschen.[670] Der Rechteinhaber sei somit selbst in der Lage, mit technisch einfachen Mitteln urheberrechtsverletzende Inhalte zu löschen.[671]

Auch das LG München I bezweifelte, dass eine geeignete Filtersoftware existiere, mit der die Inhalte, die der Cache-Provider im Usenet übermittelt und im Rahmen dessen zwischenspeichert, zeitnah und zuverlässig durchsucht werden können.[672] Zudem stellt das Gericht auf die potentielle Wirksamkeit einer solchen

[665] OLG Düsseldorf, MMR 2008, 254, 255.
[666] OLG Düsseldorf, MMR 2008, 254, 256.
[667] OLG Düsseldorf, MMR 2008, 254, 256.
[668] OLG Düsseldorf, MMR 2008, 254, 256.
[669] OLG Düsseldorf, MMR 2008, 254, 256.
[670] OLG Düsseldorf, MMR 2008, 254, 256.
[671] OLG Düsseldorf, MMR 2008, 254, 256.
[672] LG München I, MMR 2007, 453, 456.

Maßnahme ab und kommt hier zu dem Ergebnis, dass diese durch einen Zugriff über andere Newsserver mit geringem Aufwand umgangen werden könnten.[673]

cc) Bewertung der bisherigen Rechtsprechung

Den Ausführungen des OLG Düsseldorf und LG München I ist dem Grunde nach zuzustimmen, sie gelangen zu einem interessengerechten Ergebnis. Der Cache-Provider ist, nachdem er Kenntnis über eine bestimmte Urheberrechtsverletzung erlangt hat, zwar in der Lage, das urheberrechtswidrige Material von seinem Server zu entfernen, es ist ihm jedoch nicht zumutbar, im Anschluss daran jegliches Material, welches er über sein System zu einem Nutzer durchleitet, daraufhin zu überprüfen, ob es mit dem bereits beanstandeten Material übereinstimmt.

Dass Ergebnis, zu dem die beiden Gerichte kommen, lässt sich allerdings auch in Übereinstimmung mit europarechtlichen Vorgaben, und zwar mit der konsequenten Anwendung der Privilegierung des § 9 TMG, erreichen.

Eine entsprechende konsequente Anwendung des § 9 TMG ist auch für den Rechteinhaber nicht nachteilig. Ihm stehen einfache Mittel zur Verfügung, die jeweiligen rechtsverletzende Inhalte auf dem Ursprungsserver entfernen zu lassen. Diese Entfernung am Ursprungsort ist auch im Interesse des Rechteinhabers, da hierdurch die Inhalte endgültig entfernt werden und nicht durch Nutzung eines anderen Newsservers erneut abgerufen werden können.

Abzulehnen ist jedenfalls die Auffassung des LG München I, dass eine händische Überprüfung des Datenverkehrs oder Abschaltung des Usenet-Servers dann verhältnismäßig sei, wenn alle bzw. der Großteil der im Usenet vorhandenen Inhalte rechtswidrig wären.[674] Eine entsprechende händische Überprüfung des Usenet-Servers ist bereits nicht praktikabel, da es sich bei dem Usenet um ein weltweites Netzwerk mit Millionen von Inhalten handelt. Die

[673] LG München I, MMR 2007, 453, 456.
[674] LG München I, MMR 2007, 453, 456.

Inhalte liegen nicht, wie im Falle des Host-Providers, auf den eigenen Servern des Cache-Providers, sondern auf den Servern anderer Newsserver. Sie werden erst nach Nutzeranfrage zur Übermittlung zwischenzeitlich auf dem Server des Cache-Providers gespeichert. Die Überprüfung sämtlicher auf diese Weise zum Zwecke der Durchleitung gespeicherten Inhalte, wäre ab einer gewissen Nutzeranzahl nicht mehr zumutbar.
Zudem ist schon nicht feststellbar, bei wie vielen der Inhalte des gesamten Usenets es sich um rechtswidrige handelt.
Selbst wenn man zu dem Ergebnis kommt, dass ein großer Teil der Inhalte des Usenet rechtswidrig ist, lässt dies wohl kaum eine Abschaltung des Usenet-Servers des Cache-Providers rechtfertigen. Das Gericht übersieht hier, dass selbst nach Abschaltung des eigenen Newsservers die Inhalte weiterhin auf anderen Newsservern zur Verfügung stehen und auch abgerufen werden können. Das LG München I hat hier offensichtlich eine vorschnelle Aussage getroffen, ohne eingehender über die Besonderheiten und die Funktionsweise des Usenets nachzudenken.

dd) Zumutbare Prüfpflichten nach Kenntnis - „post-Stiftparfum“

Es ist fraglich, ob die Rechtsprechung der unterinstanzlichen Gerichte bezüglich des Cache-Providers nach der Stiftparfum-Entscheidung des BGH noch aufrechterhalten werden kann.
Wie unter C.I.5.b)gg)(6) dargelegt, ist die neuere Rechtsprechung des BGH zur Störerhaftung des Host-Providers als teilweise Abkehr von seiner bisherigen Rechtsprechung zu werten. Entsprechend prüft der BGH die Privilegien des § 10 TMG auch im Bereich der Unterlassungsansprüche, hält allerdings weiter an einer Prüfpflicht im Rahmen der Störerhaftung nach erstmaliger Kenntnis einer Rechtsverletzung fest. Das Ergebnis ist, dass der Host-Provider nicht, wie § 10 S. 1 Nr. 2 TMG vorschreibt, privilegiert ist, sofern er nach Kenntnis einer Rechtsverletzung diese entfernt bzw. den Zugang zu ihr sperrt, sondern die

Privilegierung wird an ein weiteres Kriterium, nämlich das Nicht-Verletzen einer Prüfpflicht, geknüpft.

Diese Rechtsprechung lässt sich allerdings nicht auf den Cache-Provider übertragen. Denn anders als bei dem Host-Provider ist dieser nach § 9 S. 1 Nr. 5 TMG nur verpflichtet, das urheberrechtsverletzende Material zu entfernen, sofern dies auch auf dem Ursprungs-Server gelöscht wurde. Dies hat schlicht den Hintergrund, dass der Cache-Provider selbst keinen Einfluss auf die Inhalte hat, die an anderer Stelle online gestellt werden. Er antwortet lediglich auf Nutzeranfragen und übermittelt in dieser Funktion das gewünschte Material und speichert dieses für einen kurzen Zeitraum.

Würde man eine wie auch immer geartete Prüfpflicht des Cache-Providers nach Kenntnisnahme einer spezifischen Rechtsverletzung als gegeben ansehen, so müsste sich diese nicht nur an einer prinzipiellen Zumutbarkeit orientieren, sondern zudem davon abhängig sein, dass das Material auf dem Ursprungs-Server gelöscht wurde.

ee) Bewertung

Eine Prüfpflicht des Cache-Providers ist grundsätzlich auf den konkret abgemahnten Inhalt, über den der Cache-Provider in Kenntnis gesetzt wurde, zu beschränken. Die Auferlegung einer weitergehenden Prüfpflicht würde eine weitere Voraussetzung schaffen, die der Cache-Provider zu erfüllen hätte, um in den Genuss der Haftungsprivilegien zu gelangen. Die Voraussetzungen der ISP-spezifischen Haftungsprivilegien sind jedoch grundsätzlich als abschließend anzusehen, so dass das Hinzufügen weiterer Voraussetzungen ausgeschlossen ist.[675] Dies würde auch dem Ziel des europäischen Gesetzgebers klar zuwider laufen.

Entsprechend trifft den Cache-Providers lediglich die Pflicht, sicherzustellen, dass der maßgeblich urheberrechtsverletzende Inhalt auf dem Server des Cache-Providers entfernt wurde. Diese

[675] So auch Szpunar, Schlussanträge vom 16.03.2016, Rn. 97 hinsichtlich der Privilegierung des Access-Providers gem. Art. 12 ECRL.

Verpflichtung ließe sich auch mit einer entsprechenden Unterlassungsklage durchsetzen, womit Art. 8 Abs. 3 InfoSoc-RL, nach dem gerichtliche Anordnungen gegen Mittelspersonen möglich sein müssen, Genüge getan wäre.

ff) Rechtsfolgen

Die Haftung des Cache-Providers als Störer begründet regelmäßig einen Beseitigungs- und Unterlassungsanspruch. Ob hierdurch auch ein sekundärer Schadensersatzanspruch begründet werden kann, ist fraglich.

(1) Beseitigungs- und Unterlassungsanspruch, § 97 Abs. 1 UrhG

Wie bereits unter C.II.1.b)ff)(1) ausgeführt, begründet die Haftung als Störer einen Beseitigungs- und Unterlassungsanspruch des Urheberrechtsinhabers. Voraussetzung hierfür ist das Vorhandensein einer Wiederholungsgefahr.

Nach der Rechtsprechung des BGH zum Host-Provider fehlt es bei derjenigen Verletzungshandlung, die eine Prüfpflicht des Host-Providers begründet, an einer solchen Wiederholungsgefahr, hierfür ist eine vollendete Verletzung nach Begründung der Prüfpflichten im Rahmen der Störerhaftung notwendig.[676] Die für den Unterlassungsanspruch notwendige Wiederholungsgefahr wird entsprechend erst durch eine erneute Rechtsverletzung nach Kenntnis über eine derartige Rechtsverletzung begründet. Im Rahmen dessen hat das Gericht jedoch zu prüfen, ob der Host-Provider überhaupt gegen die Prüfpflichten verstoßen hat und er entsprechend als Störer haftet, d.h. ob er ihm zumutbare Maßnahmen zur Verhinderung derartiger Rechtsverletzungen getroffen hat.

Diese Rechtsprechung lässt sich nicht direkt auf den Cache-Provider übertragen. Zunächst ist die Privilegierung des Cache-Providers nicht lediglich an die Kenntnis über eine spezifische Rechtsverletzung geknüpft, sondern zusätzlich daran, dass diese

[676] BGH GRUR 2011, 1038, 1042.

Rechtsverletzung am Ausgangsort der Übertragung aus dem Netz entfernt wurde. Eine Prüfpflicht des Cache-Providers nach Kenntnis einer Rechtsverletzung ist daher auf den konkret abgemahnten rechtsverletzenden Inhalt zu beschränken. Dies bedeutet, dass den Cache-Provider nach Kenntnis über einen urheberrechtsverletzenden Inhalt sowie nach Entfernung oder Sperrung des Inhalts am Ausgangsort eine Prüfpflicht lediglich dahingehend trifft, den Inhalt von seinem Server zu entfernen und damit sicherzustellen, dass er dort nicht mehr auffindbar ist. Löscht er den Inhalt nicht, so kann er auf Entfernung und Unterlassung verurteilt werden, allerdings lediglich im Hinblick auf den konkret beanstandeten Inhalt, über den er Kenntnis hatte.
Im Einklang mit § 9 S. 1 Nr. 5 TMG kann ein Gericht oder eine Verwaltungsbehörde die Entfernung und Sperrung auch dann anordnen, wenn der urheberrechtsverletzende Inhalt am Ausgangsort noch vorhanden ist.

(2) Schadensersatzanspruch, § 97 Abs. 2 UrhG

Fraglich ist, ob auch eine Schadensersatzpflicht besteht.
Sofern der Cache-Provider Kenntnis über eine spezifische Rechtsverletzung hat und diese nicht entfernt oder den Zugang zu dieser sperrt, trifft ihn zunächst nur eine durchsetzbare Unterlassungsverpflichtung.
Wie bereits beim Host-Provider wäre eine Schadensersatzpflicht denkbar, wenn der Cache-Provider rechtswidriges Urheberrechtsmaterial in vorwerfbarer Weise nicht entfernt, obwohl er positive Kenntnis hiervon hat und dieses am Ausgangsort entfernt bzw. gesperrt wurde. Geht man davon aus, dass die Störerhaftung dem Cache-Provider ab dem Zeitpunkt der Kenntnis im Sinne des § 9 S. 1 Nr. 5 TMG eine Pflicht zur Entfernung bzw. Sperrung auferlegt, so ist es denkbar, dass aus der Störerhaftung eine Haftung als Täter erwächst, nachdem der Cache-Provider sich in voller Kenntnis der Rechtswidrigkeit des streitgegenständlichen Inhalts und dessen Löschung bzw. Sperrung am Ausgangsort weigert, diesen zu entfernen.

Der entsprechende Inhalt könnte dem Cache-Provider dann als eigener Inhalt zugerechnet werden, für den er nicht mehr nach § 9 TMG privilegiert ist. Der Cache-Provider hätte den urheberrechtsverletzenden Inhalt aufgrund einer bewussten Entscheidung als Teil seines eigenen Dienstes in sein Leistungsangebot aufgenommen. Dies gilt insbesondere vor dem Hintergrund, dass der Inhalt auf dem Ursprungsserver nicht mehr zur Verfügung steht, sondern lediglich noch auf dem Server des Cache-Providers. Der Inhalt wäre ihm folglich als eigener zuzurechnen, für den er als Täter wegen schuldhafter Verletzung des Urheberrechts auch Schadensersatz i.S.d. § 97 Abs. 2 UrhG zu leisten hätte.

c) Ergebnis

Der Cache-Provider ist in der Regel nicht als Täter oder Teilnehmer verantwortlich, sofern er nicht willentlich an einer Rechtsverletzung mitgewirkt hat. Ihn kann jedoch eine Verantwortlichkeit als Störer auf Unterlassung treffen.

Sowohl die den Cache-Provider treffende Prüfpflicht nach Kenntnis über eine Rechtsverletzung sowie deren Entfernung am Ausgangsort als auch eine gerichtliche Anordnung auf Unterlassung gegen den Cache-Provider sind im Einklang mit § 9 TMG jedoch auf die Sperrung bzw. Entfernung der spezifischen urheberrechtsverletzenden Information zu beschränken.

Dies hat zum einen seine Berechtigung darin, dass der Cache-Provider gem. § 9 S. 1 Nr. 5 TMG lediglich zu einer Entfernung bzw. Sperrung verpflichtet ist, sofern er entweder Kenntnis von der Entfernung bzw. Sperrung des urheberrechtsverletzenden Materials am Ursprungsort hat oder aber dies von einem Gericht oder einer Verwaltungsbehörde angeordnet wird. Würde nun durch die Störerhaftung eine weitergehende Pflicht begründet, durch die der Cache-Provider nach Kenntnis über eine bestimmte Rechtsverletzung nicht nur verpflichtet wäre, den spezifischen Inhalt von seinem Server zu entfernen, sondern auch noch dafür Sorge tragen müsste, dass dieser Inhalt nicht wieder auf seine

Server kommt, würde dies im Widerspruch zu § 9 S. 1 Nr. 5 TMG und dem Erfordernis der Löschung auf dem Ursprungsserver bzw. einer entsprechenden gerichtlichen Anordnung stehen. Der Cache-Provider müsste zur Privilegierung noch eine weitere Voraussetzung erfüllen.
Zum anderen würde eine solche Prüfpflicht zusätzlich eine allgemeine Überwachungsverpflichtung i.S.d. § 7 Abs. 2 S. 1 TMG darstellen. Denn um etwaige zukünftige Rechtsverletzungen aufzudecken, müsste der Cache-Provider sämtliche Inhalte, die er zur Übermittlung an seine Nutzer zwischenspeichert prüfen.
Dies dürfte der intendierten Vollharmonisierung durch die ECRL zuwiderlaufen.

4. Strafrechtliche Verantwortlichkeit des Cache-Providers

Eine strafrechtliche Haftung des Cache-Providers wird aufgrund des fehlenden vorsätzlichen Handelns regelmäßig nicht gegeben sein. Da der Cache-Provider in aller Regel nicht als Täter bzw. Teilnehmer eingestuft werden kann, entfällt damit auch eine strafrechtliche Verantwortlichkeit.

5. Zivilrechtliche Verantwortlichkeit des Access-Provider

Auch der Access-Provider kann nach den allgemeinen Gründsätzen als Täter, Teilnehmer oder Störer einer Urheberrechtsverletzung haften.

a) Täter/Teilnehmer

Eine Einordnung des Access-Providers als Täter ist ihm Rahmen seiner originären, klassischen Tätigkeit, nämlich dem Bereitstellen der technischen Infrastruktur zur Übermittlung von fremden Informationen bzw. der Zugangsvermittlung, regelmäßig ausgeschlossen. Für diese neutrale Tätigkeit wird er entsprechend auch von § 8 TMG privilegiert.
Eine Verantwortlichkeit als Teilnehmer für die Durchleitung fremder Informationen käme lediglich in Fällen in Betracht, in denen der Access-Provider absichtlich mit dem Nutzer

zusammenarbeitet um eine urhebeberrechtswidrige Handlung zu begehen. Eine solche Beihilfe ist aber äußerst unwahrscheinlich.

b) Störer

Eine Haftung des Access-Providers wäre allerdings als Störer denkbar.

Hier ist insbesondere die Möglichkeit von Sperranordnungen gegen Access-Provider im Rahmen der Störerhaftung von Bedeutung.

aa) EuGH-Urteil zu Sperrverfügungen

2014 nahm der EuGH Stellung zu der Frage, ob dem Access-Provider eine gerichtliche Anordnung auferlegt werden kann, eine bestimmte Webseite zu sperren, auf der urheberrechtlich geschützte Werke ohne Zustimmung der Rechteinhaber öffentlich zugänglich gemacht werden. Das Gericht führte aus, dass Art. 8 Abs. 3 InfoSoc-RL dahingehend auszulegen sei, dass der Access-Provider auch dann als Vermittler anzusehen sei, dessen Dienste von einem Dritten zur Verletzung eines Urheberrechts genutzt werden, wenn er Zugang zu einer Seite mit urheberrechtsverletzenden Inhalten vermittle, auch wenn der Rechtsverletzer selbst nicht die Dienste des Access-Providers in Anspruch nehme.[677] Es sei ausreichend, dass durch die Dienste des Access-Providers die Kunden des Access-Providers auf die urheberrechtsverletzenden Inhalte zugreifen könnten, eines tatsächlichen Zugriffs bedürfe es nicht.[678]

Die Grundrechte der Union würden einer gerichtlichen Anordnung nicht entgegenstehen, die keine Angaben dazu enthält, welche Maßnahmen der Access-Provider ergreifen muss, um der Anordnung zur Sperrung des Zugangs einer Webseite, nachzukommen.[679] Voraussetzung ist allerdings, dass er Beugestrafen wegen eines Verstoßes gegen die Anordnung durch einen Nachweis abwenden kann, dass er alle zumutbaren Maßnahmen ergriffen hat.[680] Der Wesensgehalt der

[677] EuGH, GRUR 2014, 468, 470 (Rn. 40).
[678] EuGH, GRUR 2014, 468, 470 (Rn. 38).
[679] EuGH, GRUR 2014, 468, 472 (Rn. 64).
[680] EuGH, GRUR 2014, 468, 472 (Rn. 64).

unternehmerischen Freiheit des Access-Providers sei nicht angetastet, da er selbst, unter Beachtung der ihm zur Verfügung stehenden Ressourcen, die konkreten Maßnahmen bestimmen könne, die zur Erreichung des angestrebten Ziels zu treffen sind.[681] Grundsätzlich seien bei einer solchen Anordnung die widerstreitenden Grundrechte zu beachten und gegeneinander abzuwägen.[682] Die Maßnahmen des Access-Providers müssten hinreichend wirksam sein, um Zugriffe auf die urheberrechtlich geschützten Werke zu verhindern oder zumindest zu erschweren.[683] Zudem dürfe den Internetnutzern nicht unnötig die Möglichkeit vorenthalten werden, auf rechtmäßige Inhalte zuzugreifen.[684]

bb) Bewertung EuGH-Rechtsprechung

Das Urteil des EuGH erfuhr insbesondere hinsichtlich der Verlagerung der Grundrechtsabwägung auf den Access-Provider Kritik.[685] Eine gerichtliche Anordnung ohne jegliche Vorgaben hinsichtlich der zu treffenden Maßnahmen bedeutet für den Access-Provider ein erhebliches Maß an Rechtsunsicherheit und damit entgegen der Auffassung des EuGH einen erheblichen Eingriff in seine unternehmerische Freiheit. Er ist bei der Auswahl der Maßnahmen dazu angehalten, sowohl die Informationsfreiheit der Nutzer nicht unnötig zu beeinträchtigen als auch die Sicherung der Rechte der Urheber sicherstellen. Auch die Möglichkeit der nachträglichen Verteidigung im Rahmen des Vollstreckungsverfahrens vermag die ursprüngliche Eingriffsintensität nicht zu heilen. Es kann insoweit lediglich ein nachträgliches Gleichgewicht zwischen den Grundrechten wiederhergestellt werden.[686] Das Gleichgewicht der Grundrechte

[681] EuGH, GRUR 2014, 468, 471 (Rn. 52).
[682] EuGH, GRUR 2014, 468, 471 (Rn. 47).
[683] EuGH, GRUR 2014, 468, 471 (Rn. 62).
[684] EuGH, GRUR 2014, 468, 472 (Rn. 63).
[685] Marly, GRUR 2014, 472, 473; Nazari-Khanachayi, GRUR 2015, 115, 210; Spindler, GRUR 2014, 826, 829.
[686] So auch Villalón, BeckEuRS 2013, 743182, Rn. 85 ff.

sollte aber bereits beim Erlass der Anordnung ausreichend beachtet werden.[687]

cc) BGH-Entscheidung

In zwei Entscheidungen, denen ein fast identischer Sachverhalt zugrunde lag, hat auch der BGH zur Frage der Störerhaftung des Access-Providers und damit einhergehender Prüfpflichten Stellung genommen.[688] Es ging insbesondere um die Frage, ob der Access-Provider verpflichtet ist, als Störer den Zugang zu einer Seite zu sperren, welche Links zu urheberrechtlichen Inhalten bereithält. In der Ausgangssituation hatte ein Tonträgerhersteller ein Telekommunikationsunternehmen, das seinen Kunden Zugang zum Internet vermittelte, zur Sperrung des Zugriffs auf eine Webseite aufgefordert, die Links zu urheberrechtlich geschützten Werken, an denn der Tonträgerhersteller die Rechte hielt, zum direkten Download bereithielt. Das Telekommunikationsunternehmen kam dieser Sperrungsanordnung des Tonträgerherstellers nicht nach.

Der I. Zivilsenat führte zunächst aus, dass der Access-Provider grundsätzlich als Störer hafte.[689] Durch die Vermittlung des Zugangs zum Internet leiste er einen adäquat-kausalen Beitrag zur Rechtsverletzung, da seine Dienste an jeder Übertragung zwingend beteiligt seien und somit zur Begehung einer Urheberrechtsverletzung genutzt werden würden.[690] Ihm obliege zwar keine allgemeine Prüfungspflicht aufgrund des § 7 Abs. 2 S. 1 TMG, der Überwachungspflichten allgemeiner Art ausschließt.[691] Eine zumutbare Prüfpflicht treffe ihn aber, nachdem er auf eine konkrete Rechtsverletzung hingewiesen worden sei.[692] Zur Beurteilung der Zumutbarkeit sei eine Vereinbarkeit der Zugangssperre mit den betroffenen Grundrechten, sowohl im

[687] Villalón, BeckEuRS 2013, 743182, Rn. 88.
[688] BGH I ZR 174/14, Urteil vom 26.11.2015 – „Goldesel“ = GRUR 2016, 268; BGH I ZR 3/14, Urteil vom 26.11.2015 – „3dl.am“ = MMR 2016, 188. Aufgrund der fast identischen Urteilsbegründung wird nachstehend lediglich Bezug auf das „Goldesel“-Urteil genommen.
[689] GRUR 2016, 268, Rn. 23.
[690] GRUR 2016, 268, Rn. 25.
[691] GRUR 2016, 268, Rn. 15.
[692] GRUR 2016, 268, Rn. 27.

Hinblick auf die Charta der Grundrechte der Europäischen Union[693] als auch dem deutschen Grundgesetz, zu prüfen.[694] Entsprechend seien die grundrechtliche Gewährleistung des Eigentums gem. Art. 17 Abs. 2 EU-Grundrechtecharta und Art. 14 Abs. 1 GG, das Recht auf unternehmerische Freiheit gem. Art. 16 EU-Grundrechtecharta, das Rechte der Berufsfreiheit gem. Art. 12 Abs. 1 GG sowie das Recht auf Informationsfreiheit gem. Art. 11 Abs. 1 EU-Grundrechtecharta und Art. 5 Abs. 1 S. 1 GG gegeneinander abzuwägen.[695]

Der BGH kommt zu dem Schluss, dass der durch den Access-Provider aufzubringende administrative, technische und finanzielle Aufwand nicht gegen eine Zumutbarkeit der Durchsetzung einer Sperrverfügung spricht, da dieser bereits über die erforderlichen technischen Vorrichtungen verfüge und eine Beschaffung zusätzlicher Hardware nicht erforderlich sei.[696]

Eine Beeinträchtigung der Informationsfreiheit der Nutzer durch Overblocking sei zwar nicht ausgeschlossen, allerdings hinzunehmen, sofern es sich bei der Betrachtung des Gesamtverhältnisses von rechtmäßigen zu rechtswidrigen Inhalten um eine nicht ins Gewicht fallende Größenordnung von betroffenen legalen Inhalten handele.[697] Zudem müssten die Nutzer des Access-Providers die Möglichkeit haben, ihre von der Sperrmaßnahme betroffenen Rechte auf Informationsfreiheit vor Gericht geltend zu machen.[698] Dies sei dadurch gewährleistet, dass die Nutzer ihre Rechte gegenüber dem Access-Provider auf Grundlage des zwischen ihnen bestehenden Vertragsverhältnisses geltend machen könnten.[699]

Auch spreche nicht gegen eine Zumutbarkeit, dass DNS- bzw. IP-Sperren vom Nutzer umgangen werden könnten und daher den

[693] EU-Grundrechtecharta.
[694] GRUR 2016, 268, Rn. 31 ff.
[695] GRUR 2016, 268, Rn. 35 ff.
[696] GRUR 2016, 268, Rn. 37 ff.
[697] GRUR 2016, 268, Rn. 55.
[698] GRUR 2016, 268, Rn. 57.
[699] GRUR 2016, 268, Rn. 57.

Zugriff lediglich erschwerten.[700] Es sei nicht notwendig, dass Rechtsverletzungen vollständig abgestellt werden.[701]

Der BGH sah zudem das Fernmeldegeheimnis gem. Art. 10 Abs. 1 GG und die Achtung der Kommunikation gem. Art. 7 EU-Grundrechtecharta als nicht verletzt an.[702] Diesbezüglich führt er zunächst aus, dass Art. 10 Abs. 1 GG jeden nicht-öffentlichen Austausch konkreter Kommunikationsteilnehmer schütze.[703] An die Allgemeinheit gerichtete Kommunikation sowie die bloße Verhinderung von Kommunikation würden aus dem Schutzbereich herausfallen.[704] Die Zugangssperren stellten alleine Maßnahmen der Kommunikationsverhinderung dar und die Kenntnisnahme von Umständen der Kommunikation beschränke sich alleine auf das zur Unterbrechung Erforderliche.[705] Sofern die betroffenen Daten unmittelbar nach Erfassung technisch wieder anonym, spurenlos und ohne weitergehendes Erkenntnisinteresse gelöscht werden würden, komme den Sperren nicht die Qualität eines Eingriffs in Art. 10 Abs. 1 GG zu.[706] Zudem komme ein Eingriff nicht in Betracht, sofern die betroffenen Daten ohnehin zur Herstellung der jeweiligen Verbindung benötigt würden, da in diesem Fall § 88 Abs. 3 S. 1 TKG greife.[707] Danach ist es rechtmäßig, wenn sich der Diensteanbieter für die geschäftsmäßige Erbringung von Telekommunikationsdiensten einschließlich des Schutzes seiner technischen Systeme, Kenntnis vom Inhalt oder der näheren Umstände der Telekommunikation Kenntnis verschafft.

Auch das Grundrecht auf Achtung der Kommunikation gem. Art. 7 EU-Grundrechtecharta betreffe lediglich vertrauliche Kommunikation, die an bestimmte Adressaten und nicht die

[700] GRUR 2016, 268, Rn. 48.
[701] GRUR 2016, 268, Rn. 48 mit Bezug auf EuGH, GRUR 2014, 468, Rn. 62 f.
[702] GRUR 2016, 268, Rn. 60 ff.
[703] GRUR 2016, 268, Rn. 65.
[704] GRUR 2016, 268, Rn. 65.
[705] GRUR 2016, 268, Rn. 69.
[706] GRUR 2016, 268, Rn. 69.
[707] GRUR 2016, 268, Rn. 69.

Öffentlichkeit gerichtet sei.[708] Daher würde dieses auch nicht durch die Sperrmaßnahme tangiert werden.[709]

Der Senat ist der Auffassung, dass es für die Anordnung einer URL-Sperre auch keiner spezialgesetzlichen Grundlage bedürfe, da im Verhältnis zwischen zwei gleichgeordneten Grundrechtsträgern mit der aus § 1004 BGB richterrechtlich abgeleiteten Störerhaftung eine hinreichende Rechtsgrundlage gegeben sei.[710] Aus unionsrechtlicher Sicht sei die Frage des Gesetzesvorbehaltes entsprechend zu beantworten.[711]

Ferner spreche der Schutz der personenbezogenen Daten der Nutzer gem. Art. 8 EU-Grundrechtecharta sowie das Recht auf informationelle Selbstbestimmung aus Art. 1 i.V.m. Art. 2 Abs. 1 GG, welches seine einfachgesetzliche Ausprägung in den §§ 91 ff. TKG findet, nicht gegen die Zumutbarkeit der Sperranordnungen, sofern die IP-Adressen der Nutzer lediglich im Einklang mit § 95 TKG verwendet werden würden.[712] Die Verwendung der IP-Adresse als Bestandsdatum wäre danach zulässig, soweit dies zum Zwecke der inhaltlichen Ausgestaltung des Vertragsverhältnisses über Telekommunikationsleistungen erfolge.[713] Auch eine Verwendung zur Vermeidung von Urheberrechtsverletzungen wäre legitim, sofern eine entsprechende vertragliche Bestimmung in den Allgemeinen Geschäftsbedingungen des Access-Providers enthalten wäre.[714] Auch sei von einer zulässigen Verwendung auszugehen, wenn dem Kunden im Vertrag die Pflicht auferlegt worden wäre, den Abruf rechtswidriger Angebote zu unterlassen.[715]

Letzten Endes sah der BGH die Sperranordnung jedoch als unzumutbar an, da der Access-Provider nicht gegen den Betreiber der Webseite vorgegangen sei.[716] Denn auch wenn die Störerhaftung gegenüber der Inanspruchnahme des Täters nicht

[708] GRUR 2016, 268, Rn. 70.
[709] GRUR 2016, 268, Rn. 70.
[710] GRUR 2016, 268, Rn. 71 ff.
[711] GRUR 2016, 268, Rn. 75.
[712] GRUR 2016, 268, Rn. 76.
[713] GRUR 2016, 268, Rn. 79.
[714] GRUR 2016, 268, Rn. 79.
[715] GRUR 2016, 268, Rn. 79.
[716] GRUR 2016, 268, Rn. 81.

subsidiär sei, so sei im Rahmen der Prüfung der Zumutbarkeit darauf abzustellen, ob der Urheberrechtsinhaber gegen die vorrangig an der Rechtsverletzung Beteiligten vorgegangen sei.[717]

dd) Bewertung der BGH-Rechtsprechung

Die Rechtsprechung des BGH zur Sperrverpflichtung des Access-Providers wirft einige Fragen und Ungereimtheiten auf. Die Argumentationslinie wird daher in der Folge analysiert.

(1) Störerhaftung

Der BGH ist zunächst korrekterweise davon ausgegangen, dass der Access-Provider ein Diensteanbieter im Sinne des § 8 Abs. 1 S. 1 TMG ist. Seine Dienste werden zudem für eine Urheberrechtsverletzung im Sinne des Art. 8 Abs. 3 InfoSoc-RL genutzt.[718] Art. 8 Abs. 3 InfoSoc-RL wurde nicht explizit umgesetzt, da der Gesetzgeber davon ausging, dass die deutsche Störerhaftung diesem Genüge tut. Da dem Access-Provider jedoch gem. § 7 Abs. 2 S. 1 TMG keine allgemeinen Überwachungspflichten auferlegt werden dürfen, entsteht eine Prüfpflicht des Access-Providers nach Ansicht des erkennenden Senats im Hinblick auf die Vermittlung des Zugangs, erst nach Erhalt eines vorherigen Hinweises auf eine konkrete Rechtsverletzung.

Der I. Zivilsenat orientiert sich hier offensichtlich an die im Rahmen der Haftung des Host-Providers ergangene Rechtsprechung. Dies ist fragwürdig vor dem Hintergrund, dass sich die zu dem Host-Provider getätigten Ausführungen nicht ohne Weiteres auf den Access-Provider übertragen lassen, da es sich um zwei völlig unterschiedliche Geschäftsmodelle handelt.[719] Erhält der Host-Provider einen Hinweis über eine Rechtsverletzung, so kann er diesem Hinweis unproblematisch nachkommen, indem er das beanstandete urheberrechtsverletzende Material aus seinem

[717] GRUR 2016, 268, Rn. 82 f.
[718] Diesbzgl. wird vereinzelt im Schrifttum kritisiert, dass der Vermittlerbegriff uferlos ausgeweitet werde. So bspw. Marly, GRUR 2014, 472, 473; Spindler, GRUR 2014, 826, 828.
[719] So auch Szpunar, Schlussanträge vom 16.03.2016, Rn. 99.

Dienst entfernt. Diese Verpflichtung trifft ihn im Rahmen des § 10 TMG.

Erhält nun aber der Access-Provider einen entsprechenden Hinweis auf eine Rechtsverletzung, ist vollkommen unklar, wie er hierauf reagieren soll. Den Access-Provider trifft im Rahmen des § 8 TMG keine entsprechende Verpflichtung zur Entfernung oder Sperrung des Inhaltes. Vielmehr spricht in § 8 TMG von jeglicher Verantwortlichkeit frei, sofern er die dort festgeschriebenen Kriterien erfüllt. Hintergrund dieser unterschiedlichen Regelungen in § 8 TMG und § 10 TMG ist, dass die Rechtverletzung sich nicht auf dem Server des Access-Providers befindet und er nicht die Möglichkeit hat, die Rechtsverletzung ohne Weiteres zu entfernen oder zu sperren.

Da das vorliegende Urteil eine Anordnung zur Sperrung behandelte, scheint der Senat davon auszugehen, dass nach entsprechendem Hinweis mit entsprechender Aufforderung zur Sperrung, der Access-Provider dieser Aufforderung im Rahmen seiner ihn treffenden Prüfpflicht nachzukommen hat. Dies würde folglich bedeuten, dass der Access-Provider aufgrund eines einzigen Hinweises ein gesamtes Internetangebot, wie bspw. eine bestimmte Webseite, sperren müsste. Denn der Access-Provider kann nicht einen bestimmten rechtsverletzenden Inhalt auf der Webseite eines Dritten entfernen. Er kann lediglich den Zugang hierzu für seine Nutzer sperren. Dies kann nach derzeitigem Stand der Technik entweder durch eine DNS-Sperre, eine IP-Sperre oder eine URL-Sperre geschehen.[720] Allen Sperren gemeinsam ist, dass sie nicht lediglich die Sperrung eines einzigen, als rechtsverletzend beanstandeten Inhaltes bewirken können, sondern, dass der gesamte unter einer bestimmten IP-Adresse oder URL enthaltene Inhalt gesperrt wird.

Eine solche Pflicht erscheint abwegig und dürfte sich aus zwei verschiedenen Gründen als problematisch darstellen. Zum einen würde dem Access-Provider eine zusätzliche Voraussetzung

[720] Zu den verschiedenen Sperren siehe S. 17.

auferlegt, die er zu erfüllen hat, um eine Privilegierung gem. § 8 TMG in Anspruch zu nehmen. § 8 TMG nennt abschließend die Voraussetzungen zur Privilegierung des Access-Providers. Diese ist unabhängig von einer etwaigen Kenntnis von einer Rechtsverletzung. Den Mitgliedsstaaten ist es untersagt, dem Access-Provider weitere Voraussetzungen aufzuerlegen, um die Privilegierung in Anspruch zu nehmen. So führt auch der Bundestag in der Begründung des WLAN-Gesetzes aus, dass der Wortlaut des Art. 12 ECRL bzw. § 8 TMG weitere Voraussetzungen und Prüfpflichten für deren Anwendung ausdrücklich ausschließt.[721]

Zum anderen kann vom Access-Provider gem. Art. 12 Abs. 3 ECRL zwar durch ein nationales Gericht oder eine Verwaltungsbehörde verlangt werden, die Rechtsverletzung abzustellen oder zu verhindern und gem. Art. 8 Abs. 3 InfoSoc-RL eine gerichtliche Anordnung gegen den Access-Provider ergehen. Eine solche gerichtliche Anordnung kann aber erst ergehen, nachdem der Access-Provider gegen die ihn treffende Prüfpflicht verstoßen hat. Die Prüfpflicht trifft den Access-Provider nach Auffassung des BGH bereits nachdem er von einem Rechtsinhaber auf eine konkrete Rechtsverletzung hingewiesen wurde. Erst wenn er diese verletzt, hat der Rechteinhaber einen durchsetzbaren Unterlassungsanspruch gegen den Access-Provider als Störer. Teil des Problems ist hier auch die ungenaue Umsetzung des Art. 12 Abs. 3 ECRL durch § 7 Abs. 2 S. 2 TMG. Während die europäische Richtlinie von der Möglichkeit ausgeht, dass ein Gericht oder eine Verwaltungsbehörde anordnen kann, die Rechtsverletzung abzustellen oder zu verhindern, spricht die deutsche Vorschrift allgemein von einer Verpflichtung zur Entfernung und Sperrung nach den allgemeinen Gesetzen. Folge hiervon ist, dass der Access-Provider im Zweifel damit rechnen muss, seinen Prüfpflichten nicht in möglicher und zumutbarer Weise nachgekommen zu sein. Ist dies der Fall, kann er von einem

[721] BT-Drucks. 18/8645, S. 10.

Gericht auf Unterlassung verklagt werden kann, mit der Folge, dass ihm auch die Abmahnkosten und die gerichtlichen Kosten auferlegt werden. Gerade diese Rechtsfolge soll § 8 TMG jedoch verhindern.[722]

Auch wenn die Prüfpflicht, welche nach den Ausführungen des BGH offensichtlich identisch mit einer Sperrverpflichtung ist, den Access-Provider nur trifft, sofern diese für ihn zumutbar ist, führt dies zu weiteren Unsicherheiten seitens des Access-Providers. Für den Access-Provider ist die Frage der Zumutbarkeit schwer zu beantworten. Er weiß also im Vorhinein nicht, ob er seinen Prüfpflichten nachgekommen und damit einer potentiellen Haftung entgangen ist oder nicht. Der BGH stellt indes Kriterien auf, die zur Beurteilung, ob eine Maßnahme für den Access-Provider zumutbar ist, herangezogen werden sollen. Damit der Access-Provider folglich nicht Gefahr läuft, auf Unterlassung in Anspruch genommen zu werden, müsste er zuvor selbst anhand dieser vom BGH entwickelten Kriterien prüfen, ob eine Sperrung für ihn zumutbar ist. Hierzu müsste er aber beispielsweise prüfen, ob die Webseite, welche den beanstandeten Inhalt hostet, rechtsverletzendes Material in dem Umfang enthält, dass eine entsprechende Sperrung gerechtfertigt erscheint. Dies würde im Endeffekt auf eine umfassende Nachforschungs- und Erkundungspflicht der entsprechenden Angebote der Webseite sowie anschließende Evaluierungspflicht des Access-Providers hinauslaufen, die für ihn kaum möglich, geschweige denn ihm zuzumuten ist. Denn der Access-Provider müsste hierfür nicht lediglich das als rechtsverletzend beanstandete Material ausfindig machen, sondern müsste die anderen Inhalte der Webseite auf ihre Rechtmäßigkeit hin überprüfen. Nur so wäre es ihm möglich, eine entsprechende Einschätzung vorzunehmen. Er kann im Zweifel aber nicht wissen, ob bestimmte Inhalte bspw. mit Zustimmung des Rechteinhabers eingestellt wurden oder ohne dessen Zustimmung. Eine entsprechende Einschätzung ist daher im Zweifel nicht

[722] So auch BT-Drucks. 18/8645, S. 10.

möglich. Auch bei Internetportalen, deren Geschäftsmodell offensichtlich auf die Verletzung von Urheberrechten ausgelegt ist, müsste der Access-Provider zunächst die dort enthaltenen Dateien auf ihre Rechtmäßigkeit hin kontrollieren. Da die Inhalte eines solchen Portals aber im sechsstelligen Bereich liegen können[723], wäre eine entsprechende Überprüfung durch den Access-Provider kaum zu bewerkstelligen. Ohne eine entsprechende Einschätzung, weiß der Access-Provider aber nicht vorher, ob und in welcher Weise ein Gericht eine entsprechende Prüfpflicht als möglich oder zumutbar erachtet, und ist daher einer erheblichen Rechtsunsicherheit ausgesetzt.

Die Störerhaftung des Access-Providers ist momentan auch Gegenstand eines Verfahrens vor dem EuGH.[724] Der Generalstaatsanwalt führte diesbezüglich in seinen Schlussanträgen aus, dass Anordnungen gegen Access-Provider zwar grundsätzlich möglich seien, betonte aber gleichzeitig, dass die Voraussetzungen des Art. 12 Abs. 1 ECRL für eine Haftungsprivilegierung des Access-Providers abschließend seien und der Erlass einer gerichtlichen Anordnung nicht die Feststellung irgendeiner Haftung des Access-Provider für die Übermittlung von Informationen beinhalten dürfe.[725] Art. 12 Abs. 1 ECRL schließe jegliche Verurteilung eines Access-Providers wegen der durch die Übermittlung von Inhalten begangenen Urheberrechtsverletzungen aus.[726] Zwar könne gem. Art. 12 Abs. 3 ECRL ein Gericht bzw. eine Verwaltungsbehörde dem Access-Provider bestimmte Verpflichtungen im Rahmen einer Anordnung auferlegen, der Access-Provider könne aber nicht dafür haftbar gemacht werden, dass er eine mögliche Rechtsverletzung nicht aus eigener Initiative verhindere oder gegen eine ihm obliegende Verpflichtung eines *bonus pater familias* verstoßen habe.[727] Art. 12 ECRL verbiete die

[723] Kino.to hatte Anfang 2001 beispielsweise mehr als 1 Millionen Links zu verschiedenen Inhalten, siehe LG Leipzig, ZUM 2013, 338, 339.
[724] EuGH Rechtssache C-484-14 - Tobias Mc Fadden.
[725] Szpunar, Schlussanträge vom 16. März 2016, Rn. 86.
[726] Szpunar, Schlussanträge vom 16. März 2016, Rn. 90.
[727] Szpunar, Schlussanträge vom 16. März 2016, Rn. 79.

Geltendmachung sonstiger Geldforderungen, die die Feststellung einer Haftung des Access-Providers für Urheberrechtsverletzungen durch die Übermittlung von Informationen impliziert, wie bspw. die Erstattung gerichtlicher und außergerichtlicher Kosten.[728]

Zudem wies er korrekterweise ausdrücklich darauf hin, dass eine entsprechende Anwendung von Art. 14 Abs. 1 lit. b) ECRL auf Access-Provider nicht zulässig sei.[729] Art. 12 bis 14 ECRL behandelten verschiedene Arten von Tätigkeiten, die an unterschiedliche Voraussetzungen, abhängig von der jeweiligen Tätigkeit des ISP, anknüpften.[730]

Folgt der EuGH diesen Schlussanträgen, so steht die Rechtsprechung des BGH den europarechtlichen Vorgaben entgegen. Denn der deutsche Gerichtshof wendet nicht nur die deutsche Rechtsprechung zur Verantwortlichkeit des Host-Providers regelwidrig und ungeachtet der spezifischen Privilegierungsvoraussetzungen der §§ 8-10 TMG auf den Access-Provider an, sondern schafft durch die, wie auch immer geartete, auferlegte Prüfpflicht nach Kenntnis einer Rechtsverletzung eine zusätzliche Voraussetzung, welche der Access-Provider zu erfüllen hat, um die Privilegierung des § 8 TMG in Anspruch nehmen zu können. Die Geltendmachung einer gerichtlichen Unterlassungsanordnung wird davon abhängig gemacht, dass der Access-Provider gegen die ihn treffenden Prüfpflichten verstößt. Durch einen entsprechenden Verstoß haftet er schließlich als Störer und hat somit auch die damit einhergehenden gerichtlichen und außergerichtlichen Kosten zu tragen. Genau dies steht aber nach der hier vertretenen Auffassung im Widerspruch zu den europäischen Vorgaben.

Im Schrifttum wird vereinzelt die Auffassung vertreten, dass die Störerhaftung in ihrer aktuellen Ausgestaltung mit dem Erfordernis eines adäquat kausalen Verursachungsbeitrags gänzlich ungeeignet für den Access-Provider sei, da das europäische Recht keine

[728] Szpunar, Schlussanträge vom 16. März 2016, Rn. 74.
[729] Szpunar, Schlussanträge vom 16. März 2016, Rn. 104.
[730] Szpunar, Schlussanträge vom 16. März 2016, Rn. 99.

Kausalität voraussetzt.[731] Die deutsche Störerhaftung sei daher europarechtskonform auszulegen.[732]

(2) Grundrechtsabwägung

Fraglich sind auch die Ausführungen bzgl. der Bewertung der Gefahr des Overblocking. Der erkennende Senat bezieht sich auch hier auf die für den Host-Provider ergangene Rechtsprechung, nach der es einer Erfüllung von Prüfpflichten grundsätzlich nicht entgegensteht, wenn es im Einzelfall zur Löschung rechtmäßiger Inhalte kommt.[733] Die Schlussfolgerung, dass folglich auf das Gesamtverhältnis von rechtmäßigen zu rechtswidrigen Inhalten abzustellen sei, gelangt in seinem Kern zwar durchaus zu einem erwünschenswerten Ergebnis, völlig offen ist aber, wie der Access-Provider ein solches Gesamtverhältnis bestimmen soll. In der Praxis würde diese vom BGH verlangte Abstellung auf das Gesamtverhältnis bedeuten, dass der Access-Provider nach Erhalt eines Hinweises auf eine Urheberrechtsverletzung im Rahmen einer Grundrechtsabwägung zunächst herausfinden muss, welcher prozentuale Anteil des Gesamtangebotes legale Inhalte enthält. Denn der BGH führt aus, dass den Access-Provider nachdem er auf eine klare Rechtsverletzung hingewiesen wurde, anlassbezogene Prüfpflichten treffen.[734] Dies zwar nur sofern diese Prüfpflichten zumutbar sind. Teil dieser Zumutbarkeitsprüfung stellt lt. BGH aber unter anderem die Grundrechtsabwägung dar. Um folglich zu verhindern, dass eine Unterlassungsklage gegen den Access-Provider angestrebt wird, muss der Access-Provider ihm zumutbare Maßnahmen treffen. Und um beurteilen zu können, was für ihn zumutbar ist, müsste er zuvor selbst die Grundrechte gegeneinander abwägen.

---

[731] So bspw. Czychowski/Nordemann, GRUR 2013, 986, 989 f.; Nordemann, ZUM 2014, 499, 499 f.; insoweit auch zweifelnd: Leistner/Grisse, GRUR 2015, 19, 20.
[732] Czychowski/Nordemann, GRUR 2013, 986, 989; Nordemann, ZUM 2014, 499, 500; Leistner/Grisse, GRUR 2015, 19, 20.
[733] GRUR 2016, 268, Rn. 55.
[734] GRUR 2016, 268, Rn. 27.

Auch die Feststellung, dass der Internetnutzer im Falle einer Sperrung zulässiger Inhalte seine Rechte auf Grundlage des Vertragsverhältnisses mit dem Access-Provider gerichtlich geltend machen könne, ist nicht gänzlich durchdacht.

Der BGH verkennt, dass eine Inanspruchnahme durch den Nutzer nicht immer ohne Weiteres möglich ist. So besteht zum einen für den Access-Provider keine vertragliche Pflicht die Abrufbarkeit aller grundsätzlich vorhandenen Angebote zu gewährleisten.[735] Zudem kann sich der Access-Provider diesbezüglich auch in seinen AGB weitgehend absichern. Letzten Endes ist die Annahme, dass ein Nutzer, der im Vertragsverhältnis mit einem Access-Provider steht, im Falle der Nichtaufrufbarkeit einer spezifischen Seite, gerichtlich gegen den Access-Provider vorgehen wird, realitätsfern und lediglich theoretischer Natur. Der ungewisse Ausgang eines solchen Verfahrens und die potentiell damit verbundenen Kosten werden den Nutzer in der Regel von einer gerichtlichen Inanspruchnahme des Access-Providers abhalten.

(3) Effektivität der Sperrmaßnahmen

Nicht zu beanstanden ist, dass es der Effektivität einer Sperrmaßnahme grundsätzlich nicht entgegen steht, wenn diese den unerlaubten Zugriff auf die gegenständlichen Schutzgegenstände nicht vollkommen verhindert, sondern lediglich erschwert. Dies steht auch im Einklang mit der Rechtsprechung des EuGH. [736]

(4) Eingriff in das Fernmeldegeheimnis, Achtung der Kommunikation

Fehlerhaft sind zunächst die Ausführungen des erkennenden Senats hinsichtlich des Schutzbereichs des Art. 10 Abs. 1 GG. Zwar hat der Senat richtigerweise dem Schutzbereich des Art. 10 Abs. 1 GG lediglich nicht-öffentliche Individualkommunikation zugeordnet, so dass eine an die Allgemeinheit gerichtete Kommunikation aus dem Anwendungsbereich herausfällt. Allerdings hat er verkannt, dass im Bereich des Internetzugangs sowohl

[735] Siehe hierzu S. 216.
[736] EuGH, GRUR 2014, 468, 472 (Rn. 62 f.).

Individualkommunikation als auch Massenkommunikation stattfinden kann und dass eben zur jeweils konkreten Einordnung eine Anknüpfung an den Inhalt der jeweils übermittelten Information erforderlich ist.[737] Deshalb ist nach Auffassung des BVerfG bereits die Speicherung der den Internetzugang als solchen betreffenden Daten als Eingriff zu sehen, auch wenn sie die Angaben über die aufgerufenen Internetseiten nicht enthalten.[738]

Auch die weitergehende Begründung, dass der Schutzbereich des Art. 10 Abs. 1 GG auch insoweit nicht betroffen sei, da keine weitergehende Sichtung und Auswertung der Daten erfolge, ist fraglich. Der Senat bezieht sich hier auf das BVerfG, welches angeblich einen Grundrechtseingriff verneine, sofern die Erfassung von Fernmeldevorgängen lediglich technikbedingt erfolge und diese umgehend anonym, spurenlos und ohne Erkenntnisinteresse ausgesondert werden. Das BVerfG führt aber auch explizit aus, dass bereits die Erfassung selbst einen Eingriff in Art. 10 Abs. 1 GG darstellt.[739] Zudem gilt das Vorhergesagte nach Ausführungen des BVerfG lediglich sofern die Erfassung ungezielt geschieht.[740] Die Erfassung bei Einsetzen einer URL-Sperre, durch welche der gesamte Datenverkehr überprüft wird, erfolgt aber gerade nicht ungezielt, sondern zielt darauf ab, bestimmte Seiten für den Nutzer zu sperren. Zudem ist fraglich, ob die Daten tatsächlich anonym, spurenlos und ohne Erkenntnisinteresse umgehend gelöscht werden. Auch die weitergehende Ausführung des Senats, dass sofern die Daten ohnehin zur Herstellung der jeweiligen Verbindung benötigt werden würden, ein Eingriff gem. § 88 Abs. 3 S. 1 TKG schon nicht in Betracht käme, begegnet erheblichen Bedenken. Denn gem. § 88 Abs. 3 S. 2 TKG darf der Access-Provider die erlangten Kenntnisse lediglich für die Erbringung der

[737] BVerfG, NJW 2010, 833, 836 (Rn. 192).
[738] BVerfG, NJW 2010, 833, 836 (Rn. 192); der BGH bezieht sich hier größtenteils auf einen Aufsatz von Durner aus dem Jahr 2010 (ZUM 2010, 833), welcher augenscheinlich die im selben Jahr ergangene Rechtsprechung des BVerfG nicht berücksichtigt.
[739] BVerfG, NJW 2000, 55, 59.
[740] BVerfG, NJW 2000, 55, 59.

Telekommunikationsdienste verwenden. Es darf bezweifelt werden, dass die Sperrung von Internetseiten hierunter fällt.[741]

(5) Fehlende spezialgesetzliche Grundlage

Den Ausführungen des BGH, dass es keiner spezialgesetzlichen Grundlage für die Anordnung einer URL-Sperre für den Fall bedarf, dass man einen Eingriff in das Fernmeldegeheimnis bejahen sollte, können gute Argumente entgegen gesetzt werden. Zwar ist es so, dass Art. 19 Abs. 1 GG lediglich im Verhältnis zwischen Staat und Bürger gilt, allerdings geht der Senat mit keinem Wort auf das sog. kleine Zitiergebot des § 88 Abs. 3 S. 3 TKG ein, welcher das spezialgesetzliche Pendant zu Art. 19 Abs. 1 GG darstellt. Es bestimmt, dass eine Verwendung der durch die geschäftsmäßige Erbringung von Telekommunikationsdiensten erlangten Kenntnisse für andere Zwecke nur zulässig ist, soweit das TKG oder eine andere gesetzliche Vorschrift dies vorsieht und sich dabei ausdrücklich auf Telekommunikationsvorgänge bezieht. Auch wenn es in neuerer Zeit vereinzelt Stimmen gibt, die auch das kleine Zitiergebot lediglich im Bereich der staatlichen Eingriffsverwaltung anwendbar sehen[742], so wäre eine Auseinandersetzung hiermit wünschenswert und auch erforderlich gewesen. Insbesondere da der Gesetzgeber und die wohl h.M. das kleine Zitiergebot auch im Bereich privatrechtlicher Eingriffe für anwendbar hält.[743]

---

[741] So auch Frey/Rudolph/Oster, MMR-Beilage 2012, 1, 15.

[742] So bspw. OLG Köln, GRUR 2014, 1081, 1087, allerdings mit der Einschränkung, dass diese Vorschrift lediglich *„in erster Linie für die staatliche Eingriffsverwaltung Geltung beansprucht“*, sie aber *„doch die aus Sicht der Verfassung bestehende besondere Schutzwürdigkeit des Fernmeldegeheimnisses“* zeigt und daher der in dieser Vorschrift *„zum Ausdruck kommende, besondere Schutz des Fernmeldegeheimnisses gegen Eingriffe staatlicher Gewalt auch im Rahmen der Anwendung und Auslegung der Grundsätze der Störerhaftung zu berücksichtigen“* ist und deshalb auch eine Maßnahme, die in einem zivilrechtlichen Verfahren zwischen Privaten angeordnet wird, *„angesichts des Gewichts des in Rede stehenden Grundrechts einer ausdrücklichen und eindeutigen gesetzlichen Grundlage bedarf“*; Durner, ZUM 2010, 833, 837.

[743] BT-Drucks. 16/5048, S. 39, wo hinsichtlich des neu eingefügten Auskunftsanspruchs des § 101 UrhG auf Art. 10 GG und § 88 TKG verwiesen wird und durch Abs. 10 ausdrücklich auf das Zitiergebot Bezug genommen; Eckhardt in Spindler/Schuster, § 88 TKG, Rn. 35; Bock in BeckTKG-Kommentar, § 88, Rn. 37.

(6) Eingriff in den Schutz personenbezogener Daten - Recht auf informationelle Selbstbestimmung

Fragwürdig ist auch die Schlussfolgerung, dass der Schutz personenbezogener Daten und das Recht auf informationelle Selbstbestimmung nicht gegen eine Sperranordnung sprechen würden, sofern hierfür lediglich IP-Adressen der Nutzer im Einklang mit § 95 TKG verwendet werden würden. Hier übersieht der BGH bereits, dass eine entsprechende Zuordnung von IP-Adressen nicht unumstritten ist. Im Gegenteil, sowohl der erste und dritte Senat des BGH als auch das BVerfG und die h.M. der Literatur gehen davon aus, dass es sich jedenfalls im Bereich der dynamischen IP-Adressen regelmäßig um Verkehrsdaten i.S.d. § 96 TKG handelt und nicht um Bestandsdaten i.S.d. § 95 TKG.[744] Dem Nutzer, der sich über einen Access-Provider in das Internet einwählt, wird regelmäßig eine dynamische IP-Adresse zugeteilt. Lediglich die Webseite, auf der die Linksammlungen gespeichert sind, verfügt über eine statische IP-Adresse. Die datenschutzrechtliche Zulässigkeit der Erhebung und Verwendung der IP-Adressen der Nutzer beurteilt sich entsprechend nicht nach § 95 TKG sondern nach § 96 TKG, welcher, wie der erkennende Senat selbst ausführt, eine wesentlich strengere Regelung darstellt. Nach dieser Vorschrift dürfen die Verkehrsdaten grundsätzlich nur für das Herstellen und Aufrechterhalten einer Kommunikationsverbindung erhoben werden. Eine Verwendung ist gleichermaßen lediglich zulässig, sofern dies für das Herstellen bzw. das Aufrechterhalten der Kommunikationsverbindung sowie für durch andere gesetzliche Vorschriften begründete Zwecke erforderlich ist. Es darf bezweifelt werden, dass die Erhebung und Nutzung der IP-Adressen im Rahmen der Sperrung von Internetseiten zum Schutz von Urheberrechten hierunter fällt. Der BGH hätte sich zumindest mit dieser Frage auseinander setzen

[744] BVerfG, NJOZ 2011, 1492, Rn. 21; BGH NJW 2012, 2958, 2961; BGH MMR 2011, 341, 344; Spindler in Spindler/Schuster, § 101 UrhG, Rn. 21; Dreier in Dreier/Schulze, § 101 UrhG, Rn. 35; Karg, MMR-Aktuell 2011, 315811.

müssen, verpasst dies aber, indem er pauschal auf § 95 TKG abstellt.

Aber auch die Ausführungen zu § 95 TKG, nach welchem Bestandsdaten zum Zwecke der inhaltlichen Ausgestaltung eines Vertragsverhältnisses über Telekommunikationsleistungen erhoben und verwendet werden dürfen, können zurecht hinterfragt werden. So sieht der erkennende Senat eine Nutzung der IP-Adresse zur Vermeidung von Urheberrechtsverletzungen als zulässig an, sofern er sich dies vertraglich durch eine entsprechende Generalklausel, bspw. in Allgemeinen Geschäftsbedingungen, gestatten lässt.[745] Diese Interpretation ist vor allem vor dem Gesichtspunkt bedenklich, dass sich der Access-Provider hiernach weitreichende Befugnisse durch entsprechende Aufnahme in AGB einräumen lassen kann, da hierdurch die Voraussetzung für die inhaltliche Ausgestaltung des Vertragsverhältnisses geschaffen werden. Die inhaltliche Ausgestaltung eines Vertragsverhältnisses über Telekommunikationsdienstleistungen sollte sich aber vielmehr an der jeweiligen Telekommunikationsleistung an sich orientieren und nicht an hiervon unabhängigen anderen Leistungen. Hierzu gehört beispielsweise die Bereitstellung eines Telekommunikationsdienstes, die ordnungsgemäße Abwicklung des Zahlungsverkehrs, die Beseitigung von technischen Störungen oder die Bearbeitung von Kundenbeschwerden.[746] Es darf bezweifelt werden, dass nur weil eine bestimmte Befugnis des Access-Providers in dessen AGB geregelt wird, dies zugleich dazu führt, dass diese Befugnis als für die inhaltliche Ausgestaltung erforderlich angesehen werden kann.

Auch sofern der BGH ausführt, dass von einer Verwendung der Daten zur Durchführung des Vertrags auszugehen ist, wenn dem Kunden vertraglich die Pflicht auferlegt wird, den Abruf rechtswidriger Angebote zu unterlassen, verkennt das Gericht, dass es bspw. im vorliegenden Fall durchaus umstritten ist, ob die streitgegenständliche Webseite, welche lediglich Links zu

[745] GRUR 2016, 268, Rn. 79.
[746] Büttgen in Beck'scher TKG-Kommentar, § 95 Rn. 5.

urheberrechtlich geschützten Werken bereithält, als rechtswidriges Angebot angesehen werden kann. [747]

(7) Vorhergehende Inanspruchnahme vorrangig Beteiligter

Zuzustimmen ist dem BGH dahingehend, dass die Störerhaftung gegenüber der Inanspruchnahme des Täters nach geltender Rechtslage nicht subsidiär ist. Dass der Senat dennoch aus der Tatsache, dass der Rechteinhaber nicht zunächst in erschöpfender Art und Weise gegen den Betreiber der Webseite mit den Linksammlungen vorgegangen ist, auf eine Unzumutbarkeit der Sperrung für den Access-Provider herleitet, kann wohl als subsidiäre Haftung über Bande gewertet werden.

(8) Ergebnis

Der I. Zivilsenat ist auf einem holprigen Weg zu einem wünschenswerten Ergebnis gelangt. Das Kernproblem liegt dabei in der deutschen Störerhaftung und den damit einhergehenden Prüfpflichten. Dass den Access-Provider nach Kenntnis über eine bestimmte Rechtsverletzung Prüfpflichten treffen, steht den Vorgaben des Unionsrechts entgegen. Der Access-Provider hat auf europäischer Ebene die umfassendste Haftungsprivilegierung erfahren. Eine gerichtliche Anordnung gegen den Provider muss allerdings in Übereinstimmung mit europäischen Vorgaben, genauer gesagt Artikel 8 Abs. 3 InfoSoc-RL, möglich sein. Im Rahmen dieser Anordnung hat das Gericht dann umfassend die Zumutbarkeit und technischen Möglichkeiten des Access-Providers zur Sperrung zu beleuchten. Gelangt das Gericht zu dem Ergebnis, dass es dem Access-Provider zumutbar und möglich ist eine spezifische Webseite zu sperren, hat das Gericht eine entsprechende Anordnung zu erlassen. Der Access-Provider sollte aber nicht dazu verpflichtet sein, selbst eine entsprechende Zumutbarkeitsprüfung durchzuführen und ggf. eine Webseite zu sperren aufgrund eines vorherigen Hinweises eines Rechteinhabers.

[747] Zur Verantwortlichkeit des Linksetzenden siehe S. 181.

Dies würde für den Access-Provider ein hohes Maß an Unsicherheit bedeuten.

c) Zivilrechtliche Verantwortlichkeit des WLAN-Anbieters

Nach der Rechtsprechung des BGH zum privaten WLAN-Betreiber als auch der unterinstanzlichen Rechtsprechung zu gewerblichen WLAN-Betreibern können diese grundsätzlich aufgrund von Urheberrechtsverletzungen Dritter als Störer haften.[748]

Während der BGH für den Inhaber eines privaten WLAN-Anschlusses eine automatisch eintretende Prüfpflicht in Form einer marktüblichen Sicherung bei Inbetriebnahme des WLAN sieht[749], entschied das AG Berlin-Charlottenburg in scheinbarem Widerspruch hierzu, dass demjenigen, der seinen WLAN-Anschluss im Rahmen der Freifunk-Initiative Dritten zur freien Verfügung stellen will, keine Prüfpflichten auferlegt werden dürften, die das Geschäftsmodell des WLAN-Betreibers gefährdeten, wie bspw. Port- und DNS-Sperren oder aber auch Registrierungs- und Belehrungspflichten[750].

Auch hinsichtlich Art und Umfang der Prüfpflichten gewerblicher WLAN-Anbieter besteht Uneinigkeit. Während ein Teil der Gerichte im Rahmen der Störerhaftung ab dem Zeitpunkt der Inbetriebnahme des offenen WLAN-Anschlusses eine Prüfpflicht dahingehend sehen, dass der Zugang gegenüber dem unberechtigten Zugriff Dritter zu verschlüsseln sei und die Nutzer auf die Einhaltung gesetzlicher Vorschriften zu verpflichten seien[751], zweifelte ein anderer Teil bereits an einer Belehrungspflicht hinsichtlich des Verbots rechtswidriger Nutzungen[752]. Vereinzelt wurde sogar eine Pflicht zur Sperrung von einzelnen für das Filesharing erforderlichen Ports als zumutbar angesehen.[753]

---

[748] Siehe hierzu S. 96 und S. 98.
[749] BGH GRUR 2010, 633, 635.
[750] AG Berlin-Charlottenburg, GRUR-RS 2015, 02858.
[751] AG Hamburg, BeckRS 2014, 13884; LG Frankfurt, MMR 2011, 401, 402.
[752] AG Hamburg, BeckRS 2014, 13884; AG Hamburg, ZUM-RD 2015, 207, 209.
[753] LG Hamburg, MMR 2011, 475, 475.

Im Gegensatz hierzu wurde kürzlich jedoch die Unanwendbarkeit des § 8 TMG auf Unterlassungsansprüche in Zweifel gezogen, was insgesamt zu einem Verneinen von Prüfpflichten führen würde, sofern der WLAN-Betreiber die Voraussetzungen des § 8 TMG erfüllt.[754]

Auch nach in Kraft treten des WLAN-Gesetzes ist nach wie vor unklar, ob der WLAN-Betreiber als Störer in Anspruch genommen werden kann. Eine diesbezüglich eindeutige Regelung wäre wünschenswert gewesen. Klarheit hinsichtlich der gebotenen Auslegung könnte jedoch das derzeit vor dem EuGH anhängige Verfahren des LG München I bringen.[755]

aa) Rechtsfolgen

Die Haftung des Access-Providers als Störer würde Beseitigungs- und Unterlassungsansprüche nach sich ziehen. Ein Schadensersatzanspruch ist aber in der Regel ausgeschlossen.

(1) Beseitigungs- und Unterlassungsanspruch, § 97 Abs. 1 UrhG

Wie bereits unter C.II.1.a)cc)(1) ausgeführt, begründet die Haftung als Störer einen Beseitigungs- und Unterlassungsanspruch des Urheberrechtsinhabers. Voraussetzung hierfür ist das Vorhandensein einer Wiederholungsgefahr, welche nach der Rechtsprechung des BGH hinsichtlich derjenigen Verletzungshandlung, die eine Prüfpflicht begründet, nicht gegeben ist.[756] Es ist vielmehr eine vollendete Verletzung nach Begründung der Prüfpflichten im Rahmen der Störerhaftung notwendig.[757]

Nachdem der Access-Provider folglich auf eine klare Rechtsverletzung hingewiesen wurde, trifft ihn eine entsprechende Prüfpflicht.[758] Um als Störer auf Unterlassung zu haften, muss er

---

[754] LG München I, ZUM 2015, 344, 350; Andeutend bereits AG Hamburg, ZUM-RD 2015, 207, 209: *"Auch bei Vertretung der Ansicht, dass § 8 TMG (mangels unmittelbarer Anwendbarkeit) einer Inanspruchnahme als Störer nicht grundsätzlich entgegensteht [...]"*.

[755] Siehe hierzu S. 100.

[756] BGH GRUR 2011, 1038, 1042.

[757] BGH GRUR 2011, 1038, 1042.

[758] BGH GRUR 2016, 268, Rn. 27.

gegen die ihm zumutbare Prüfpflicht verstoßen haben. In den beiden hierzu vorliegenden Entscheidungen des BGH ist ein entsprechender Verstoß daran gescheitert, dass die Urheberrechtsinhaber nicht alle zumutbaren Anstrengungen unternommen haben, um gegen die Beteiligten vorzugehen, die die Rechtsverletzung entweder selbst begangen oder zu dieser durch Erbringung einer Dienstleistung vorrangig beigetragen haben.[759]
Den WLAN-Betreiber hingegen treffen nach der Rechtsprechung einiger Gerichte bereits ab Inbetriebnahme entsprechende Prüfpflichten. Die Gerichte bewerten diese Prüfpflichten unterschiedlich, generell denkbar ist eine Verschlüsselung des Zugangs oder eine Verpflichtung der Nutzer zur Einhaltung gesetzlicher Vorschriften. Verletzt er diese, kann auch er zur Unterlassung verpflichtet werden. Unklar ist auch hier, welchen Umfang eine solche Unterlassungsverpflichtung haben soll.

(2) Schadensersatzanspruch, § 97 Abs. 2 UrhG

Wie bereits unter C.II.1.a)cc)(2) erörtert, zieht die Störerhaftung grundsätzlich keinen Schadensersatzanspruch nach sich. Auch ein sekundärer Schadensersatzanspruch kann, anders als beim Host-Provider und Cache-Provider, grundsätzlich nicht ausgelöst werden, da ein zu eigen Machen der Inhalte regelmäßig fehlt. Der Access-Provider stellt lediglich die technische Infrastruktur zur Verfügung. Selbst wenn sich der Access-Provider hartnäckig weigern würde, den Zugang zu spezifischem rechtswidrigen Material zu sperren, so würde er den rechtswidrigen Inhalt dennoch nicht als eigenen Inhalt in seinen Dienst aufnehmen. Vielmehr würde er lediglich nicht den Zugang hierzu sperren, was eine Verletzung seiner Unterlassungsverpflichtung darstellen würde und entsprechend sanktioniert werden könnte.

d) Ergebnis

Eine Haftung des Access-Providers als Täter/Teilnehmer ist regelmäßig ausgeschlossen. Es kommt allerdings eine Haftung als

[759] BGH GRUR 2016, 268, Rn. 81.

Störer aufgrund eines adäquat-kausalen Beitrages des Access-Providers zu einer Urheberrechtsverletzung in Betracht.

Der I. Zivilsenat sieht die Verletzung von Prüfpflichten nach Kenntnis einer konkreten Rechtsverletzung als Voraussetzung für eine solche Störerhaftung an. Er hat hier unbedacht seine Argumentation für die Haftung des Host-Providers übernommen ohne sich eingehender mit den damit verbundenen Konsequenzen auseinanderzusetzen. Der Host-Provider hat gem. § 10 S. 1 Nr. 2 TMG das beanstandete Material zu entfernen bzw. den Zugang hierzu zu sperren hat und anschließend im Rahmen der ihn nach Kenntnis treffenden Prüfpflicht weitere Maßnahmen zu unternehmen, um zu verhindern, dass es zu erneuten Rechtsverletzungen kommt. Den Access-Provider trifft jedoch keine entsprechende Pflicht zur Entfernung bzw. Sperrung des beanstandeten Materials im Rahmen des § 9 TMG. Wenn der BGH nun also davon spricht, dass den Access-Provider eine Prüfpflicht im Hinblick auf die Vermittlung des Zugangs zu den geschützten Musikwerken treffe, deren Verletzung die Wiederholungsgefahr begründen könne, nachdem er auf eine klare Rechtsverletzung hingewiesen wurde, bedeutet dies, dass der Access-Provider den Zugang nach einer entsprechenden Kenntnis zu sperren hat. Denn nur so kann er die Vermittlung des Zugangs zu dem beanstandeten Material unterbinden. Diese Prüfpflicht, welche nach den Ausführungen des BHG offensichtlich identisch mit einer Sperrverpflichtung ist, trifft den Access-Provider allerdings nur, sofern diese für ihn zumutbar ist. Für den Access-Provider ist die Frage der Zumutbarkeit allerdings schwer selbst zu beantworten. Eine nach den Kriterien des BGH aufgestellte Prüfung ist für ihn kaum selbst durchzuführen. Ihn trifft daher eine erhebliche Unsicherheit. In der Praxis kann dies dazu führen, dass der Access-Provider auf Geheiß eines einzelnen Urheberrechtsinhabers eine komplette Webseite für seine Kunden sperren. Denn die Frage der Zumutbarkeit ist auf Seiten des Access-Providers schwer zu beantworten, dass dies im Zweifel dazu führen kann, dass er Seiten

sperrt, um hierdurch einer potentiellen Haftung zu entgehen. Diese drastische Konsequenz hat ihren Ursprung darin, dass der deutsche Gesetzgeber Art. 8 Abs. 3 InfoSoc-RL bereits in der bestehenden Störerhaftung widergespiegelt sah, so dass er von einer konkreten Umsetzung absah. Art. 8 Abs. 3 InfoSoc-RL fordert aber eine gerichtliche Anordnung und nicht eine Anordnung durch den Rechteinhaber.

Zwar ist es korrekt, dass nach den Prinzipien der Störerhaftung der Urheberrechtsinhaber eine gerichtliche Anordnung gegen den Vermittler, hier also den Access-Provider, beantragen kann, allerdings setzt eben diese Anordnung im Rahmen der Störerhaftung eine Verletzung von Prüfpflichten voraus, welche entsprechend eine Verantwortlichkeit des Access-Providers begründet.

Dies führt zu dem Ergebnis, dass die Prüfpflicht, welche ursprünglich eingefügt wurde, um die Haftung des lediglich mittelbar Beteiligten nicht über Gebühr auf Dritte zu erstrecken, im Falle des Access-Providers einer sofortigen Unterlassungspflicht nach Kenntnis über eine spezifische Rechtsverletzung gleichkommt bzw. bei Nichtbeachtung dieser Prüfpflicht eine Verantwortlichkeit des Access-Providers für die Rechtsverletzungen Dritter begründet.

Dies ist insbesondere vor dem Hintergrund der weitreichenden Folgen einer solchen Sperre misslich und es darf bezweifelt werden, dass dies im Sinne des europäischen Richtliniengebers ist. Denn auch wenn der EuGH davon ausgeht, dass eine entsprechende Sperrungsanordnung gegen den Access-Provider im Hinblick auf Artikel 8 Abs. 3 InfoSoc-RL möglich sein muss, so ist diese Sperranordnung nicht an eine etwaige Verantwortlichkeit des Access-Providers geknüpft und darf nicht dazu führen, dass diesem entsprechend die Kosten hierfür auferlegt werden.

Um zu einem für den Access-Provider gerechteren Ergebnis zu gelangen, insbesondere aufgrund seines legitimen und gesellschaftlich erwünschten Geschäftsmodells, wäre das Erfordernis einer richterlichen Anordnung zur Sperrung von

urheberrechtsverletzenden Inhalten eine wesentlich interessengerechtere Lösung. Eine solche gerichtliche Anordnung ist auch im Einklang mit Art. 12 Abs. 3 ECRL sowie Art. 8 Abs. 3 InfoSoc-RL.

6. Strafrechtliche Verantwortlichkeit des Access-Providers

Eine strafrechtliche Verantwortlichkeit des Access-Providers ist aufgrund seiner neutralen Tätigkeit grundsätzlich ausgeschlossen. Bei dem bislang einzigen strafrechtlichen Verfahren gegen einen Access-Provider wegen Zugangsvermittlung zu „harter" Pornographie im Internet wurde das Urteil des AG München[760], welches den Access-Provider aufgrund Mittäterschaft verurteilte, vom LG München I wegen fehlenden Verschuldens wieder aufgehoben.[761]

7. Zivilrechtliche Verantwortlichkeit des Linksetzenden und Suchmaschinenanbieters

Wie bereits unter C.I.5.e) ausgeführt, sind die Haftungsprivilegien nicht auf Linksetzende bzw. Suchmaschinenanbieter anwendbar. Dennoch haben sich einige Parallelen hinsichtlich der Haftung der ISP i.S.d. TMG und der Linksetzenden und Suchmaschinenbetreiber entwickelt. Ihre Haftung richtet sich aber grundsätzlich nach den allgemeinen Grundsätzen.

a) Hyperlinks und Deeplinks

Im Hinblick auf die Haftung für Hyperlinks gibt es bereits mehrere höchstinstanzliche Urteile.

aa) Paperboy-Entscheidung des BGH

In der „Paperboy"-Entscheidung hat der BGH 2003 entschieden, dass durch das Setzen eines Hyperlinks sowie Deep-Links zu einer Datei auf einer fremden Webseite mit einem urheberrechtlich geschützten Werk nicht in das Vervielfältigungsrecht oder Recht der öffentlichen Zugänglichmachung an diesem Werk eingegriffen

[760] AG München, MMR 1998, 429.
[761] LG München I, NJW 2000, 1051.

wird.[762] Der I. Zivilsenat führte aus, dass das urheberrechtliche Werk durch das Setzen eines Hyperlinks nicht i.S.d. § 16 UrhG vervielfältigt werde.[763] Ein Link stelle lediglich eine elektronische Verknüpfung zu einer anderen im Internet eingestellten Datei dar, so dass es erst nach Anklicken des Links durch den Nutzer zu einer urheberrechtlich relevanten Vervielfältigungshandlung kommen könne.[764] Auch halte derjenige, der den Link zu einem zugänglich gemachten urheberrechtlich geschütztem Werk setzt, dieses Werk nicht selbst öffentlich zum Abruf bereit oder übermittle dieses selbst auf Abruf an Dritte, da allein derjenige, der das Werk ursprünglich ins Internet gestellt hat, darüber entscheide, ob das Werk der Öffentlichkeit zugänglich bleibt.[765] Zwar werde einem Nutzer, welcher die genaue URL des urheberrechtlichen Werkes nicht kennt, der Zugang durch den Hyperlink erst ermöglicht, dies sei aber mit den Fußnoten bei einem Druckwerk vergleichbar.[766] Daher sei auch ein Eingriff in die öffentliche Zugänglichmachung als unbenanntes Recht der öffentlichen Wiedergabe aus § 15 UrhG zu verneinen.[767]

Auch eine Störerhaftung des Linksetzenden lehnte der I. Zivilsenat mit der Begründung ab, dass derjenige, der ein urheberrechtlich geschütztes Werk ohne technische Sicherungsmaßnahmen öffentlich zugänglich mache, dadurch bereits selbst die Nutzungen, die ein Abrufender vornehmen kann, ermögliche und deshalb kein urheberrechtlicher Störungszustand geschaffen werde, wenn der Zugang zu dem Werk durch das Setzen von Hyperlinks erleichtert werde.[768]

---

[762] BGH GRUR 2003, 958.
[763] BGH GRUR 2003, 958, 961.
[764] BGH GRUR 2003, 958, 961.
[765] BGH GRUR 2003, 958, 962.
[766] BGH GRUR 2003, 958, 962.
[767] BGH GRUR 2003, 958, 961 (Anm.: § 19a UrhG wurde erst wenige Wochen später, mit Wirkung vom 13.09.2003, durch das Gesetz zur Regelung des Urheberrechts in der Informationsgesellschaft in das UrhG eingefügt).
[768] BGH GRUR 2003, 958, 961.

bb) Session-ID-Entscheidung des BGH

In der „Session-ID“-Entscheidung stand der I. Zivilsenat vor der Frage, ob es einen Eingriff in das Recht der öffentlichen Zugänglichmachung des Urheberrechtsinhabers darstellt, wenn durch das Setzen eines Hyperlinks technische Schutzmaßnahmen umgangen werden. Im Einklang mit seiner „Paperboy“-Entscheidung führte der Senat zunächst aus, dass das Setzen eines Hyperlinks, auch in Form des Deep-Links, grundsätzlich keine urheberrechtliche Nutzungshandlung darstelle sofern das Werk ohne technische Schutzmaßnahmen im Internet öffentlich zugänglich gemacht wurde.[769] Sofern der Berechtigte sich allerdings technischer Schutzmaßnahmen bediente, um den Zugang zu dem urheberrechtlich geschützten Werk lediglich bestimmten Nutzern zu ermöglichen und der Linksetzende derartige Schutzmaßnahmen umging, greife dieser in das Recht der öffentlichen Zugänglichmachung des Berechtigten ein.[770] In diesem Fall eröffne der Linksetzende Nutzern den Zugang zu dem Werk, den diese ohne entsprechende Linksetzung nicht hätten.[771] Dafür bedürfe es allerdings keiner Schutzmaßnahmen i.S.d. § 95a UrhG, es reiche aus, dass durch die Schutzmaßnahmen der Wille des Berechtigten erkennbar sei, dass er den Zugang zu dem geschützten Werk nur mit der von ihm vorgesehenen Einschränkung ermöglichen wolle.[772]

cc) Svensson-Entscheidung des EuGH

Auch der EuGH bestätigte in der „Svensson“-Entscheidung, dass eine Verlinkung auf eine Webseite mit frei zugänglichen urheberrechtlichen Inhalten keine Handlung der öffentlichen Wiedergabe darstellt.[773] Zur Begründung schlug er allerdings einen anderen Weg ein als der BGH. Er verwies zunächst auf die zwei Tatbestandsmerkmale der öffentlichen Wiedergabe, nämlich einer

[769] BGH MMR 2011, 47, 48.
[770] BGH MMR 2011, 47, 48.
[771] BGH MMR 2011, 47, 48.
[772] BGH MMR 2011, 47, 49.
[773] EuGH GRUR 2014, 360, 361 - Urteil vom 13.02.2014 - C-466/12.

Handlung der Wiedergabe eines Werkes sowie einer Öffentlichkeit dieser Wiedergabe.[774] Das erste Tatbestandsmerkmal sei weit zu verstehen, hierfür reiche es aus, wenn ein Werk einer Öffentlichkeit in einer Weise zugänglich gemacht werde, dass deren Mitglieder Zugang hierzu haben.[775] Der EuGH fasst folglich auch die Bereitstellung von Links zu geschützten Werken unter die Zugänglichmachung und stuft diese deshalb als Handlung der Wiedergabe ein.[776] Auch das zweite Tatbestandsmerkmal der Öffentlichkeit sah der Gerichtshof als gegeben an, da sich die Links an sämtliche potentielle Nutzer seiner Seite richteten.[777]

Würde die Wiedergabe allerdings ein Werk betreffen, welches bereits öffentlich im Internet wiedergegeben wurde und würde dieses nach demselben technischen Verfahren erfolgen, dann läge nur dann eine öffentliche Wiedergabe vor, wenn sich die Wiedergabe durch Linksetzung an ein neues Publikum richte, also ein Publikum dass der Urheberrechtsinhaber nicht hatte erfassen wollen, als er die ursprüngliche öffentliche Wiedergabe erlaubte.[778] Sofern das Werk auf der Ursprungsseite keiner beschränkenden Maßnahme unterlag und somit für sämtliche Internetnutzer frei zugänglich war, sei dieses auch bei der Linksetzung durch einen Dritten nicht an ein neues Publikum gerichtet.[779] Dies sei auch der Fall, wenn das Werk bei Anklicken des Links durch den Internetnutzer in einer Art und Weise erscheine, die den Eindruck vermittele, dass es auf der Seite erscheint, auf der sich der Link befindet und eben nicht auf der Ursprungsseite.[780]

dd) Zwischenergebnis

Auch wenn die dogmatische Herleitung des BGH und des EuGH sich von einander unterscheiden, so gelangen beide Urteile zu dem gleichen Ergebnis. Während der BGH davon ausgeht, dass das

[774] EuGH GRUR 2014, 360, 361 (Rn. 16).
[775] EuGH GRUR 2014, 360, 361 (Rn. 17 ff.).
[776] EuGH GRUR 2014, 360, 361 (Rn. 20).
[777] EuGH GRUR 2014, 360, 361 (Rn. 21 f.).
[778] EuGH GRUR 2014, 360, 361 (Rn. 24).
[779] EuGH GRUR 2014, 360, 361 (Rn. 26).
[780] EuGH GRUR 2014, 360, 361 (Rn. 29 f.).

Setzen eines Hyperlinks grundsätzlich keine urheberrechtliche Nutzungshandlung darstellt, sondern lediglich den Zugang zu einem urheberrechtlich geschütztem Werk erleichtert, geht der EuGH im Grundsatz von einer urheberrechtlichen Nutzungshandlung i.S.d. öffentlichen Wiedergabe aus, lässt deren Anwendbarkeit aber letzten Endes daran scheitern, dass der Link, jedenfalls sofern er auf ein frei im Internet zugängliches Werk verweist, sich an kein neues Publikum richtet. Der EuGH scheint demnach maßgeblich an den Willen des Urheberrechtsinhabers anzuknüpfen, während der BGH von einem technischen Verständnis ausgeht.[781] Diese unterschiedliche dogmatische Herleitung ist vor allem unter dem Gesichtpunkt von Bedeutung, dass beide Entscheidungen von einem Sachverhalt ausgingen, bei dem das urheberrechtlich geschützte Material durch den Urheberrechtsinhaber selbst bzw. mit dessen Einwilligung im Internet öffentlich zugänglich gemacht wurde.

Eine Haftung als Täter/Teilnehmer bzw. Störer ist folglich bei der Verlinkung von rechtmäßig ins Internet eingestellten Inhalten nicht gegeben. Fraglich ist, wie der Sachverhalt zu beurteilen ist, wenn es sich um urheberrechtlich geschützte Inhalte handelt, die ohne Zustimmung des Rechtsinhabers ins Internet gestellt wurden.

Rückschlüsse können hier zunächst aus zwei BGH-Urteilen aus dem Bereich des Wettbewerbsrecht gezogen werden.

ee) Schöner Wetten-Entscheidung des BGH

In der „Schöner Wetten“-Entscheidung des I. Zivilsenats ging es um die Frage der Haftung für die Linksetzung eines Presseunternehmens im Rahmen seiner Berichterstattung auf eine Webseite mit Glücksspielen, für die das Unternehmen zwar über eine Genehmigung zur Veranstaltung von Glücksspielen in einem Mitgliedsstaat, nicht aber für Deutschland, verfügte.[782]

Der Senat sah zunächst eine Haftung als Täter nicht gegeben an, da der Linksetzer keinen eigenen Wettbewerbsverstoß beginge und

[781] So auch Jani/Leenen, GRUR 2014, 360, 362 f.
[782] BGH GRUR 2004, 693.

auch nicht in der Absicht gehandelt habe einen solchen zu fördern.[783]

Auch eine Störerhaftung lehnte das Gericht ab, da der Linksetzende keine zumutbaren Prüfpflichten verletzt habe.[784] Es führte aus, dass sich der Umfang der Prüfpflichten für das Setzen oder Aufrechterhalten eines Hyperlinks grundsätzlich nach dem Gesamtzusammenhang, in dem der Hyperlink verwendet wird, richte sowie danach, ob und wieweit der Linksetzende von einer etwaigen Rechtswidrigkeit der Webseite, auf die der Link verweist, Kenntnis habe bzw. haben musste.[785] Auch sofern bei dem Setzen eines Hyperlinks keine Prüfpflicht verletzt werde, könne eine solche noch immer während der Aufrechterhaltung verletzt werden, insbesondere nachdem der Linksetzende aufgrund einer Abmahnung oder Klageerhebung von der Rechtswidrigkeit erfahre.[786] Allerdings dürften im Interesse der Meinungs- und Pressefreiheit keine allzu strengen Anforderungen an die erforderliche Prüfung gestellt werden, sofern die Hyperlinks nur den Zugang zu ohnehin allgemein zugänglichen Quellen erleichterten.[787]

Diese Prüfpflicht sah der erkennende Senat im vorliegenden Fall als nicht verletzt an, da die Rechtswidrigkeit, welche hinsichtlich des streitgegenständlichen Webangebotes ohnehin umstritten war, ohne eingehende rechtliche Prüfung nicht erkennbar gewesen sei.[788] Auch habe sich der Linksetzende den Inhalt nicht in irgendeiner Weise zu eigen gemacht.[789]

ff) ueber18.de-Entscheidung des BGH

In der „ueber18.de“-Entscheidung entschied der I. Zivilsenat, dass derjenige, der sich die fremde Information auf die er mittels eines

[783] BGH GRUR 2004, 693, 694.
[784] BGH GRUR 2004, 693, 695.
[785] BGH GRUR 2004, 693, 695.
[786] BGH GRUR 2004, 693, 695.
[787] BGH GRUR 2004, 693, 695.
[788] BGH GRUR 2004, 693, 696.
[789] BGH GRUR 2004, 693, 696.

Hyperlinks verweist, zu eigen machen kann und somit dafür wie für eine eigene Information haftet.[790]

Der Linksetzende im vorliegenden Fall setzte auf seiner Internetseite nicht nur Hyperlinks auf Webseiten Dritter, sondern auf solche Webseiten, welche allesamt ein Altersverifikationssystem des Linksetzenden nutzten, dass gegen § 4 Abs. 2 S. 2 des Jugendmedienschutz-Staatsvertrages (JMStV) verstieß.[791] Der Linksetzende biete seinen Kunden folglich nicht nur ein unzureichendes Altersverifikationssystem an, sondern schalte das Angebot jeweils frei und nehme es anschließend in den Hyperlink-Katalog auf seiner Webseite auf.[792] Dadurch werde den Internetnutzern auf der Suche nach einschlägigen Angeboten ein gebündelter Zugang zu Webseiten Dritter verschafft, die allesamt nicht dem Erfordernis des JMStV entsprechen.[793] Die Webseite des Linksetzenden sei gerade darauf ausgerichtet, den Internetnutzer zu Webseiten Dritter mit entsprechenden Inhalten zu führen.[794] Daher unterliege die Tatsache, dass sich der Linksetzende die vermittelten Inhalte zu eigen gemacht habe, keinem Zweifel.[795]

gg) Haftung für Hyperlink-Urteil des BGH

Die Entscheidung „Haftung für Hyperlink“ des I. Zivilsenats wendet die Grundsätze, welche der BGH für die Haftung des Host-Providers entwickelt hatte, auch für den Linksetzenden an. So führt er aus, dass zur Konkretisierung der Prüfpflichten auf die vom Senat im Zusammenhang mit Host-Providern entwickelten Grundsätze zurückgegriffen werden könne.[796] Demnach dürfe dem Linksetzenden keine proaktive Überwachungspflicht auferlegt werden, da Hyperlinks für die Internetnutzer unerlässlich seien, um die unübersehbare Informationsflut des Internets zu erschließen.[797] Der Linksetzende würde, sofern der rechtsverletzende Inhalt der

[790] BGH GRUR 2008, 534, 536.
[791] BGH GRUR 2008, 534, 535.
[792] BGH GRUR 2008, 534, 536.
[793] BGH GRUR 2008, 534, 536.
[794] BGH GRUR 2008, 534, 536.
[795] BGH GRUR 2008, 534, 536.
[796] BGH GRUR 2016, 209, 212.
[797] BGH GRUR 2016, 209, 212.

verlinkten Webseite nicht deutlich erkennbar sei, für solche Inhalte grundsätzlich erst dann haften, wenn Dritte ihn über die Rechtswidrigkeit in Kenntnis setzen.[798] Im Gegensatz zum Host-Provider sei jedoch keine klare Rechtsverletzung zu verlangen, sondern den Linksetzenden treffe nach entsprechendem Hinweis eine Prüfungspflicht der verlinkten Internetseite, auch wenn es sich nicht um eine klar erkennbare Rechtsverletzung handele.[799] Als Begründung für diese Ungleichbehandlung des Linksetzenden ggü. dem Host-Provider führte der erkennende Senat die unterschiedliche Interessenlage an. Während es sich bei dem Host-Provider um ein von der Rechtsordnung gebilligte Geschäftsmodell handele, würden Hyperlinks auf kommerziellen Webseiten diesen lediglich ein zusätzliches Informationsangebot hinzufügen, das für die auf dieser Webseite angebotenen Waren oder Dienstleistungen weder essenziell wäre noch ihren Wert oder Nutzen steigere.[800] Da es sich zudem zumeist um eine begrenzte Anzahl von Hyperlinks auf der Webseite handele, sei es daher sachgerecht, das Risiko einer rechtlichen Beurteilung der verlinkten Inhalte dem Linksetzenden zuzuordnen.[801]

Erstmals hat der erkennende Senat zudem der Unterscheidung zwischen einem Verweis in Form eines Deep-Links und eines Links auf die Startseite einer spezifischen Webseite Bedeutung zugewiesen.[802] Demnach sei es insbesondere für die Prüfung des zu eigen Machens von verlinkten Inhalten von Bedeutung, dass der beanstandete Inhalt nicht bereits durch einfaches Klicken auf den Link dem Nutzer zugänglich ist, sondern erst durch weiteres Navigieren auf dem verlinkten Internetauftritt.[803]

hh) Zwischenergebnis

Überträgt man die Rechtsprechung des BGH im Bereich des Wettbewerbsrecht auf das Urheberrecht, so haftet der Linksetzende

[798] BGH GRUR 2016, 209, 212.
[799] BGH GRUR 2016, 209, 212 f.
[800] BGH GRUR 2016, 209, 212 f.
[801] BGH GRUR 2016, 209, 213.
[802] BGH GRUR 2016, 209, 211.
[803] BGH GRUR 2016, 209, 211.

in der Regel nicht als Täter oder Teilnehmer einer Urheberrechtsverletzung auf dessen Inhalt er verweist. Etwas anderes gilt nur für den Fall, dass der Linksetzende sich den Inhalt des Dritten zu eigen gemacht hat. Wann ein solches zu eigen machen vorliegt ist strittig. Teilweise wird davon ausgegangen, dass sich ein Linksetzender die Inhalte bereits dann zu eigen macht, wenn er diese mit einem Kommentar versieht, bspw. „schaut euch das mal an".[804] Lt. BGH ist für die Frage des zu eigen Machens jedenfalls die objektive Sicht eines verständigen Durchschnittsnutzers auf Grundlage einer Gesamtbetrachtung aller Umstände maßgeblich.[805]

Eine Störerhaftung kommt indes bereits in Betracht, wenn entweder die Rechtswidrigkeit des verlinkten Inhaltes klar erkennbar ist oder der Linksetzende über die Rechtswidrigkeit in Kenntnis gesetzt wurde und Prüfpflichten verletzt hat.[806] Einer proaktiven Prüfpflicht hat der BGH eindeutig eine Absage erteilt. Eine Prüfpflicht trifft auch den Linksetzenden grundsätzlich erst nach Kenntnis über eine Rechtsverletzung auf der von ihm verlinkten Seite. Im Gegensatz zum Host-Provider reicht es hier allerdings aus, wenn der Linksetzende einen Hinweis auf eine Rechtsverletzung erhält, es ist hier keine klare Rechtsverletzung vorauszusetzen. Ihn trifft durch den Hinweis die Pflicht, die verlinkte Webseite auf die behauptete Rechtsverletzung hin selbst zu prüfen. Dies gilt jedenfalls für solche Webseiten, welche über nur wenige Links im Rahmen ihres kommerziellen Auftritts verfügen.

b) Framing

Auch für den Bereich des Framing existiert bereits höchstrichterliche Rechtsprechung, sowohl auf nationaler Ebene als auch auf EU-Ebene.

[804] Solmecke in Hoeren/Sieber/Holznagel, Teil 21.1, Rn. 93.
[805] BGH GRUR 2016, 209, 211.
[806] BGH GRUR 2016, 209, 212.

aa) Die Realität-Entscheidung des BGH

Im Rahmen der „Die Realität“-Entscheidung hatte der BGH hinsichtlich der urheberrechtlichen Zulässigkeit des Framings zu entscheiden. Insbesondere ging es um die Frage, ob die Einbettung eines fremden urheberrechtlichen Werkes im Wege des Framing auf die eigene Webseite eine öffentliche Zugänglichmachung i.S.d. § 19a UrhG darstellt.[807]

Der I. Zivilsenat verneinte eine öffentliche Zugänglichmachung in Übereinstimmung mit seiner „Paperboy“-Entscheidung, da der Inhaber der fremden Webseite darüber entscheide, ob das auf seiner Webseite bereitgehaltene Werk für die Öffentlichkeit zugänglich bleibt.[808] Es komme insoweit auch nicht auf ein zu eigen Machen der Inhalte durch Einbettung an, da der Tatbestand einer urheberrechtlichen Nutzungshandlung alleine durch die Vornahme der Nutzungshandlung erfüllt werde und nicht dadurch, dass deren Merkmale vorgetäuscht werden.[809]

In der Folge setzt sich der erkennende Senat mit den vom EuGH aufgestellten Voraussetzungen einer öffentlichen Wiedergabe auseinander und stellt fest, dass das streitgegenständliche urheberrechtliche Werk nicht für ein neues Publikum wiedergegeben werde, da dieses bereits für alle Internetnutzer öffentlich zugänglich gemacht worden sei und eine Verlinkung im Wege des Framing den Kreis der potentiellen Nutzer nicht erweitere.[810] Dennoch sieht er einen Eingriff in ein unbenanntes Verwertungsrecht der öffentlichen Wiedergabe, da derjenige, der ein fremdes Werk im Wege des Framing zu einem integralen Bestandteil seiner eigenen Webseite mache, Nutzern nicht nur den Zugang zu dem Werk erleichtere, sondern sich das fremde Werk durch eine solche Einbettung in seine eigene Webseite zu eigen mache.[811] Hierdurch erspare sich derjenige, der das fremde Werk in seine Webseite einbettet, die Einholung der Zustimmung des

[807] BGH MMR 2013, 596, 597.
[808] BGH MMR 2013, 596, 597.
[809] BGH MMR 2013, 596, 597.
[810] BGH MMR 2013, 596, 598.
[811] BGH MMR 2013, 596, 599.

Rechteinhabers, weshalb ein solches Verhalten bei wertender Betrachtung als öffentliche Wiedergabe einzustufen sei.[812]
Da die Bewertung des vorliegenden Sachverhaltes jedoch von einer Auslegung des Art. 3 InfoSoc-RL abhing, wurde das Verfahren ausgesetzt, um eine Vorabentscheidung des EuGH einzuholen.[813]

bb) BestWater-Entscheidung des EuGH

Dem EuGH wurde die Frage zur Vorabentscheidung vorgelegt, ob eine Einbettung eines auf einer fremden Webseite öffentlich zugänglich gemachten fremden Werkes in die eigene Webseite unter den Umständen wie sie im Ausgangsverfahren vorliegen, eine öffentliche Wiedergabe darstellt, auch wenn das fremde Werk damit nicht für ein neues Publikum wiedergegeben wird und die Wiedergabe mittels demselben technischen Verfahren erfolgt wie die ursprüngliche Wiedergabe.[814] Dies verneinte der EuGH mit Hinweis auf seine „Svensson"-Entscheidung in lakonischer Kürze durch Beschluss.[815] Demnach sei die Verlinkung auf ein geschütztes Werk, auch im Wege des Framing, welches bereits auf einer anderen Webseite frei öffentlich wiedergegeben wurde, nur dann eine öffentliche Wiedergabe, wenn diese Wiedergabehandlung sich an ein neues Publikum richte.[816]
Dies sei insbesondere dann der Fall, wenn das Werk bereits auf einer anderen Webseite mit Erlaubnis des Urheberrechtsinhabers für alle Internetnutzer frei zugänglich sei.[817]

cc) Zwischenergebnis

Nicht aufgegriffen in seinem Beschluss hat der EuGH die Konstellation in welcher die ursprüngliche Datei, die eingebettet wird, ohne Erlaubnis des Urheberrechteinhabers ins Internet gestellt wurde. Dies ist insbesondere vor dem Hintergrund bedauerlich, dass dies wohl im Ausgangsverfahren der Fall war

[812] BGH MMR 2013, 596, 599.
[813] BGH MMR 2013, 596, 597.
[814] EuGH MMR 2015, 46, 47 - Urteil vom 21.10.2014 - C-348/13.
[815] EuGH MMR 2015, 46, 48 (Rn. 19).
[816] EuGH MMR 2015, 46, 47 (Rn. 15).
[817] EuGH MMR 2015, 46, 47 (Rn. 16).

und sich die Vorlagefrage explizit auf die Umstände, wie sie im Ausgangsverfahren vorliegen, bezieht. Der EuGH hätte sich folglich bei der Beantwortung der Vorlagefrage hiermit beschäftigen müssen. Stattdessen bezieht er sich lediglich beispielhaft auf den Fall, in dem das Werk auf einer anderen Webseite mit Erlaubnis des Urheberrechtsinhabers für alle Internetnutzer frei zugänglich ist und folgert, dass die Wiedergabe an ein neues Publikum insbesondere nicht vorliege, wenn das Werk bereits auf einer anderen Webseite mit Erlaubnis des Urheberrechtsinhabers frei zugänglich sei.[818] Es bleibt offen, welche anderen Fälle er hier durch die Einfügung dieser beispielhaften Aufzählung im Kopf hatte.

Diese Unachtsamkeit des Gerichtshofes führt dazu, dass teilweise in der Literatur pauschal davon ausgegangen wird, dass mit der Einbettung von Inhalten, die ohne Erlaubnis des Urheberrechtsinhabers eingestellt wurden, ein neues Publikum erreicht werde und daher eine öffentliche Wiedergabe vorliege.[819]

dd) Die Realität II-Entscheidung des BGH

Die Auffassung, dass mit Einbettung von Inhalten ohne Erlaubnis des Urheberrechtsinhabers ein neues Publikum erreicht wird, vertritt auch der BGH nach dem Beschluss des EuGH.[820] So führt der erkennende Senat aus, dass es sich nach der Rechtsprechung des EuGH bei der Verlinkung von Urheberrechtswerken, auch im Wege des Framing, nur dann nicht um eine Wiedergabe für ein neues Publikum handele, wenn die Werke auf der anderen Seite mit Erlaubnis des Urheberrechtsinhabers für alle Internetnutzer frei zugänglich seien.[821] Der erkennende Senat verstehe diese Rechtsprechung so, dass die verlinkten Werke in derartigen Fällen für ein neues Publikum wiedergegeben werden würden, wenn keine

[818] EuGH MMR 2015, 46, 47 (Rn. 16).
[819] So bspw. Fuchs/Farkas, ZUM 2015, 110, 117; Höfinger, ZUM 2014, 293, 295; Jani/Leenen, GRUR 2014, 362, 362; Leistner, GRUR 2014, 1145, 1154; Schulze, ZUM 2015, 106, 110; Solmecke, MMR 2015, 48, 48.
[820] BGH GRUR 2016, 171.
[821] BGH GRUR 2016, 171, 174.

entsprechende Erlaubnis des Urheberrechtsinhabers vorliege.[822] Er folgert dies u.a. aus dem Verständnis des EuGH, dass es sich bei einem neuen Publikum um ein Publikum handele, an das der Urheber nicht dachte, als er die öffentliche Wiedergabe des Werkes ursprünglich erlaubte.[823] Entsprechend könne der Urheber nicht an ein bestimmtes Publikum gedacht haben, wenn er die ursprüngliche öffentliche Wiedergabe nicht erlaubt hat und daher richte sich die Wiedergabe in diesem Fall an ein neues Publikum.[824]

Der Senat verwies die Angelegenheit an das Berufungsgericht zur Klärung der Frage, ob das streitgegenständliche Werk mit Zustimmung des Rechtsinhabers ins Internet gestellt wurde, zurück.[825]

Obwohl der BGH ausdrücklich anerkannte, dass die Frage, ob es sich um eine öffentliche Wiedergabe handele, wenn das verlinkte Werk ohne Zustimmung des Rechteinhabers ins Internet gestellt wurde, nicht unmittelbar vom EuGH beantwortet wurde, sah er von einer erneuten Vorlage an den Gerichtshof ab, da nicht ersichtlich sei, ob die in Rede stehende Frage für die abschließende Entscheidung des Berufungsgerichts überhaupt von Bedeutung sei.[826] Aus dem gleichen Grund sah er auch eine Aussetzung des Verfahrens aufgrund eines derzeit beim EuGH anhängigen Vorabentscheidungsverfahrens des *Hoge Raad der Nederlanden*[827], in welchem dem EuGH genau diese Frage zur Vorabentscheidung vorgelegt wurde, nicht veranlasst.[828]

ee) Zwischenergebnis

Die Interpretation des Begriffs des neuen Publikums des BGH in seiner Folgeentscheidung ist keineswegs zwingend. So lässt die Entscheidungsbegründung durchaus eine anderweitige Auslegung

[822] BGH GRUR 2016, 171, 174.
[823] BGH GRUR 2016, 171, 174.
[824] BGH GRUR 2016, 171, 174.
[825] BGH GRUR 2016, 171, 175.
[826] BGH GRUR 2016, 171, 175.
[827] EuGH C-160/15: Vorabentscheidungsersuchen des Hoge Raad der Nederlanden (Niederlande), eingereicht am 7. April 2015 - GS Media BV/Sanoma Media Netherlands BV u. a.
[828] BGH GRUR 2016, 171, 175.

zu. Es handelt sich nach Auffassung des EuGH durchaus nicht nur dann nicht um eine Wiedergabe für ein neues Publikum, wenn die verlinkten Werke mit Erlaubnis des Urheberrechtsinhabers für alle Internetnutzer frei zugänglich gemacht wurden, vielmehr handelt es sich *insbesondere* in einem solchen Fall um keine Wiedergabe für ein neues Publikum.[829] Hierdurch hat der Gerichtshof also keineswegs ausgeschlossen, dass eine Verlinkung auf ein Werk, welches ohne Zustimmung des Urheberrechtsinhabers öffentlich zugänglich gemacht wurde, als an ein neues Publikum gerichtet anzusehen ist.

Zudem scheint auch die Argumentation des BGH vor und nach Beschluss des EuGH im Vorabentscheidungsverfahren wenig stringent. So schien der I. Zivilsenat in „Die Realität I“ noch ohne Weiteres selbst davon auszugehen, dass durch die Verlinkung auf den streitgegenständlichen Inhalt kein neues Publikum erreicht wurde.[830] Entsprechend führte er ohne weitere Argumentation aus, dass das Werk nicht für ein neues Publikum wiedergegeben werden würde, da es bereits durch das Einstellen auf der Videoplattform für alle Internetnutzer öffentlich zugänglich gemacht wurde und somit durch Verlinkung auf der Internetseite der Kreis der potentiellen Adressaten nicht erweitert werden würde.[831]

c) Suchmaschinen-Anbieter

Auch Suchmaschinen-Anbieter verlinken auf Inhalte Dritter im Internet. Im Gegensatz zu dem Linksetzenden erfolgt die Anzeige von Links in einer Ergebnisliste jedoch automatisch aufgrund einer Suchanfrage des Nutzers.

aa) Anzeigen von Ergebnislisten auf Suchanfrage

Hinsichtlich der Haftung des Suchmaschinenanbieters für Links innerhalb generierter Ergebnislisten existiert bislang keine höchstrichterliche Rechtsprechung.

[829] EuGH MMR 2015, 46, 47 (Rn. 16).
[830] BGH MMR 2013, 596, 598.
[831] BGH MMR 2013, 596, 598.

Da die Hauptaufgabe des Suchmaschinen-Anbieters darin liegt, Hyperlinks zu anderen Inhalten aufgrund zuvor getätigter Suchanfragen des Nutzers im Internet zur Verfügung zu stellen, dürfte sich dessen Verantwortlichkeit auch nach den zuvor genannten Maßstäben für den einfachen Linksetzenden richten. Dies gilt auch bei der Anzeige sog. Snippets, das sind kurze Textauszüge aus einer Webseite, die in der Ergebnisliste einer Suchmaschine angezeigt werden.[832]

Bei der Bewertung von Prüfpflichten des Suchmaschinen-Anbieters ist allerdings besonders dessen Schlüsselfunktion für das Auffinden von Inhalten im Internet zu beachten und in die Gesamtabwägung mit einzubeziehen.[833] Aufgrund der automatischen Generierung und Anzeige einer riesigen Anzahl von Suchergebnissen ist auch der Suchmaschinenanbieter grundsätzlich nicht dazu verpflichtet, die durch eine Suchanfrage generierten Links auf rechtswidrige Inhalte zu überprüfen.[834] Eine Prüfpflicht trifft den Suchmaschinen-Anbieter erst sofern dieser ganz konkret auf eine Urheberrechtsverletzung hingewiesen wurde, so dass er die Möglichkeit hat diese aus seiner Ergebnisliste zu entfernen.[835] Entgegen der Ausführungen in der „Haftung für Hyperlink"-Entscheidung wird es dem Suchmaschinen-Anbieter entsprechend auch nicht zuzumuten sein, jedem beliebigen Hinweis auf eine Rechtsverletzung nachzugehen. Es ist hier vielmehr, analog der Grundsätze zum Host-Provider, auf eine klare Rechtsverletzung abzustellen.

Sofern das *LG Hamburg*[836] es für den Suchmaschinen-Anbieter für zumutbar erachtet, Maßnahmen zu ergreifen, um zukünftige Rechtsverletzungen des Berechtigten zu verhindern, ohne eine weitere inhaltliche Ausgestaltung einer solchen Pflicht

[832] KG, MMR 2012, 129; OLG Hamburg, MMR 2011, 685; Söder in BeckOK InfoMedienR, § 823 BGB, Rn. 26.
[833] Spindler/Volkmann in Spindler/Schuster, § 1004 BGB, Rn. 49.
[834] OLG Hamburg, MMR 2011, 685, 687; OLG Nürnberg, MMR 2009, 131, 132; Reber in BeckOK UrhG, § 97 Rn. 78.
[835] OLG München, MMR 2012, 108, Reber in BeckOK, UrhG, § 97 Rn. 78; Söder in BeckOK InfoMedienR, § 823 BGB, Rn. 25.
[836] LG Hamburg, NJW 2015, 796, 801.

vorzunehmen, sind diese Maßnahmen darauf zu beschränken, den entsprechend entfernten Hyperlink nicht mehr in der Suchergebnisliste aufzuführen. Weitergehende Maßnahmen des Suchmaschinen-Anbieters dürften unter dem Gesichtspunkt der Zumutbarkeit bereits nicht zu verlangen sein.

bb) Anzeigen von Vorschaubildern in Ergebnislisten

Der BGH hat entschieden, dass das Anzeigen von Vorschaubildern in Ergebnislisten grundsätzlich das Recht des Urhebers auf Vervielfältigung und öffentliche Zugänglichmachung berührt.[837] Allerdings sieht er eine schlichte Einwilligung in eine solche Nutzung darin, dass der Urheber bei der Einstellung des Bildes ins Internet keine entsprechende Blockierung von Suchmaschinenindexierungen vorgenommen hat.[838] Es könne von demjenigen, der das Bild öffentlich zugänglich macht, erwartet werden, von technischen Möglichkeiten Gebrauch zu machen, um die Abbildung seiner Werke von der Suche und der Anzeige in Bildersuchmaschinen in Form von Vorschaubildern zu verhindern.[839] Tue er dies nicht, so erkläre er seine Einwilligung mit der Indexierung innerhalb einer Bildersuchmaschine, welche er lediglich dadurch widerrufen könne, dass er entsprechende Sicherungen seiner Werke gegen den Zugriff von Bildersuchmaschinen vornehme.[840]

In einer zweiten Entscheidung hinsichtlich der Anzeige von Vorschaubildern durch Suchmaschinen führte der I. Zivilsenat zudem hinsichtlich des Falles aus, dass das Vorschaubild auf eine Webseite verweist, auf der das Bild rechtswidrig eingestellt wurde.[841] Es könne in diesem Fall nicht von einer wirksamen Einwilligung desjenigen ausgegangen werden, der das Werk rechtswidrig öffentlich zugänglich macht.[842] Der erkennende Senat leitet hier jedoch eine Einwilligung aus der Tatsache her, dass der

[837] BGH GRUR 2010, 628, 629.
[838] BGH GRUR 2010, 628, 632.
[839] BGH GRUR 2010, 628, 632.
[840] BGH GRUR 2010, 628, 632.
[841] BGH MMR 2012, 383 – „Vorschaubilder II“.
[842] BGH MMR 2012, 383, 384.

Rechteinhaber anderen Personen Nutzungsrechte für eine öffentliche Zugänglichmachung eingeräumt hatte und in diesem Zusammenhang auch in die Nutzung seiner Abbildung in der Bildersuchmaschine eingewilligt habe.[843] Die Suchmaschine untersuche das Internet in einem automatisierten Verfahren unter Einsatz von Computerprogrammen nach Bildern und könne daher nicht dahingehend unterscheiden, ob ein Bild von einem Berechtigten oder Nichtberechtigten ins Internet gestellt worden ist.[844] Der Betreiber einer Suchmaschine könne daher die Einwilligung in die Wiedergabe eines Bildes als Vorschaubild nach ihrem objektiven Erklärungsinhalt nur so verstehen, dass sich diese auch auf die Wiedergabe als Vorschaubild auf solche Werke erstrecke, die ohne Zustimmung des Rechteinhabers ins Internet gestellt wurden.[845]

cc) Zwischenergebnis

Die Rechtsprechung des BGH hinsichtlich der Anzeige von Vorschaubildern lässt den Willen des Senats erkennen, die Tätigkeit der Suchmaschinen-Anbieter nicht unnötig zu behindern. Während die „Vorschaubilder I"-Entscheidung durchaus auf einer dogmatisch soliden Grundlage, nämlich der einer schlichten Einwilligung, steht, kommt die Entscheidung in „Vorschaubilder II" einer „Quasi-Fair-Use-Regelung"[846] gleich. Insbesondere die Ausführungen des Senats, dass von einer wirksamen Einwilligung für die Anzeige in den Suchmaschinenergebnissen insgesamt ausgegangen werden könne, sofern der Rechteinhaber diesbezüglich auch nur eine Lizenz an einen anderen Dritten erteilt habe, führt zu der ausufernden Konstruktion einer quasi allumfassenden Einwilligung, losgelöst von der konkreten Einwilligung an einen bestimmten Lizenznehmer.[847]

[843] BGH MMR 2012, 385.
[844] BGH GRUR 2012, 383, 385.
[845] BGH GRUR 2012, 383, 385.
[846] Thum, GRUR-Prax 2012, 215, 215.
[847] So auch Spindler, MMR 2012, 386, 386 f.

dd) Rechtsfolgen

Die Haftung des Linksetzenden und Suchmaschinenanbieters könnte sowohl Beseitigungs- und Unterlassungsansprüche als auch Schadensersatzansprüche begründen.

(1) Beseitigungs- und Unterlassungsanspruch, § 97 Abs. 1 UrhG

Ein Beseitigungs- und Unterlassungsanspruch kann sich sowohl auf eine täterschaftliche Haftung durch ein zu eigen Machen der Inhalte stützen als auch auf die Störerhaftung. Voraussetzung ist bei beiden Tatformen das Vorhandensein einer Wiederholungsgefahr. Sofern der Linksetzende sich die verlinkten Inhalte zu eigen macht, begründet bereits die Verletzung des Urheberrechts die Wiederholungsgefahr. Im Rahmen der Störerhaftung bedarf es hingegen einer Kenntnis bzw. einer Verletzung von zumutbaren Prüfpflichten des Linksetzenden.[848] Entfernt der Linksetzende nach einer Abmahnung den Link von seiner Internetseite, haftet er auch nicht als Störer.[849]

Für den Fall, dass der Linksetzende einer Unterlassungsverpflichtung unterliegt, ist diese jedoch auf die Entfernung des jeweils rechtsverletzenden Links zu begrenzen.

(2) Schadensersatzanspruch, § 97 Abs. 2 UrhG

Ein Schadensersatz kommt zunächst in Fällen in Betracht, in denen der Linksetzende sich die verlinkten Inhalte zu eigen gemacht hat. Im Rahmen der Störerhaftung, wie bereits unter 1.b)ff)(2) erörtert, ist ein Anspruch auf Schadensersatz grundsätzlich nicht gegeben. Nach der neuesten Rechtsprechung des BGH wäre zudem ein Schadensersatzanspruch gegen denjenigen denkbar, der Inhalte im Wege des Framing in seine Webseite einbaut, sofern das dort eingebettete Werk ohne Zustimmung des Rechteinhabers ins Internet gestellt wurde. In diesem Fall richte sich das durch das Framing zugänglich gemachte Werk an eine neue Öffentlichkeit, weshalb derjenige, der das Werk auf seiner Seite einbettet, in das

[848] BGH GRUR 2016, 209, 213.
[849] BGH GRUR 2016, 209, 213.

Recht der öffentlichen Zugänglichmachung des Urhebers eingreife. Eine solche Haftung als Täter begründet entsprechend auch einen Anspruch auf Schadensersatz.

d) Ergebnis

Die Verantwortlichkeit für Linkssetzung ist trotz mehrfacher höchstrichterlicher Rechtsprechung noch immer nicht eindeutig geklärt. Insbesondere die neueste Rechtsprechung des I. Zivilsenates für den Bereich des Framing hat zu einer Verschärfung der bisherigen Grundsätze der Verantwortlichkeit für die Linksetzung geführt. Denn die Argumentation hinsichtlich des neuen Publikums für den Fall, dass das urheberrechtliche Werk ohne Zustimmung des Urhebers ins Internet gestellt wurde, ist nicht auf Fälle des Framings begrenzt, sondern kann auf sämtliche Linksetzungen durch Dritte übertragen werden, da sie maßgeblich auf den Begriff der öffentlichen Wiedergabe abstellt und das Erreichen eines neuen Publikums.[850] Weitergedacht würde dies bedeuten, dass jegliche Verlinkung von Inhalten eine potentielle Gefahr der Haftung für den Linksetzenden darstellt. Dieser müsste sich, bevor er einen Hyperlink auf seiner eigenen Webseite einfügt, jedes Mal dahingehend versichern, dass sich auf der verlinkten Seite kein Material befindet, welches ohne Zustimmung des Urhebers öffentlich zugänglich gemacht wurde. Streng genommen müsste er zudem laufend überwachen, ob solches Material nicht in Zukunft dort eingefügt wird. Denn auch die verschuldensunabhängige Verletzung von Urheberrechten zieht bereits Unterlassungsansprüche nach sich. Es ist folglich unbeachtlich, ob der Linksetzende überhaupt Kenntnis von einer rechtswidrigen Verwendung von urheberrechtlich geschütztem Material auf einer verlinkten Seite hatte, er würde bereits für eine Verletzung des Rechts der öffentlichen Wiedergabe haften, ohne dass ihn ein Verschulden trifft.[851]

[850] So auch Spindler, GRUR 2016, 157, 158.
[851] So auch Spindler, GRUR 2016, 157, 158.

Theoretisch wäre sogar eine Übertragung dieser Grundsätze auf den Suchmaschinenanbieter möglich.[852]

Die in der „Die Realität II"-Entscheidung aufgestellten Maßstäbe widersprechen zudem den Ausführungen im Rahmen der „Haftung für Hyperlink"-Entscheidung des gleichen Senats, in welcher dieser noch ausdrücklich davon ausging, dass der Linksetzende grundsätzlich erst haftet, wenn ihn Dritte über die Rechtswidrigkeit eines spezifischen Inhaltes in Kenntnis gesetzt haben oder sofern der rechtsverletzende Inhalt deutlich erkennbar ist. Diese Widersprüchlichkeit ist das Ergebnis des Widerwillens des I. Zivilsenats, Hyperlinks und Framing nach den gleichen Grundsätzen zu behandeln.

Grünberger schlägt daher vor, den Linksetzenden bei offensichtlicher Rechtswidrigkeit der Zugänglichmachung als Teilnehmer (Gehilfe) der öffentlichen Zugänglichmachung eines Dritten haften zu lassen oder bei Verstoß gegen zumutbare Pflichtverletzungen, als Störer.[853] Bei einer nicht offensichtlichen Rechtswidrigkeit entfalle jedoch die Verantwortlichkeit aufgrund der fehlenden bewussten Wiedergabe an ein neues Publikum.[854]

Zudem gibt die Rechtsprechung des BGH hinsichtlich der Haftung des Suchmaschinenanbieters für Vorschaubilder deutlich zu erkennen, dass diese maßgeblich davon beeinflusst ist, dass der BGH die Suchmaschinenindexierung als sozialadäquate Tätigkeit schützen will.[855] Um zu einem für diese Tätigkeit interessengerechten Ergebnis zu gelangen, entwickelt der BGH jedoch fragwürdige Konstruktionen, welche in der zukünftigen Rechtsfortentwicklung zu weiteren Unklarheiten führen dürften.[856]

[852] So auch Spindler, GRUR 2016, 157, 158.
[853] Grünberger, ZUM 2015, 273, 289.
[854] Grünberger, ZUM 2015, 273, 289.
[855] So auch Spindler, MMR 2012, 386, 386.
[856] So auch Spindler, MMR 2012, 386, 387.

8. Strafrechtliche Verantwortlichkeit des Linksetzenden und Suchmaschinenanbieters

Für den Fall, dass der Linksetzende als Täter oder Teilnehmer klassifiziert werden kann, ist auch eine strafrechtliche Verantwortlichkeit denkbar. Das LG Leipzig hat sich in einem Fall mit der strafrechtlichen Haftung des Betreibers einer Linksammlung für das öffentliche Zugänglichmachen von urheberrechtlich geschützten Inhalten auseinandergesetzt.

a) Kino.to-Urteil des LG Leipzig

Das Urteil des LG Leipzig[857] behandelte die bis 2011 größte deutschsprachige Plattform für Raubkopien von Filmwerken Kino.to. Die Plattform selbst hielt keine urheberrechtlich geschützten Werke zum Abruf bereit, Nutzer der Plattform hinterlegten dort allerdings Links, welche auf von ihnen abgelegte urheberrechtliche geschützte Inhalte bei Filehostern verwiesen.[858] Die Auswahl der Filehoster sowie der Dateien erfolgte in diesem Fall durch den Nutzer, allerdings wurden sämtliche Links erst nach manueller Prüfung durch Mitarbeiter von Kino.to (sog. „Freischaltern“) von diesen freigeschaltet, so dass sie der Öffentlichkeit zur Verfügung standen.[859] Die gesamte Plattform war darauf ausgelegt, Links zu aktuellen Kinofilmen und TV-Serien zur Verfügung zu stellen und wurde von den Betreibern der Plattform auch so beworben.[860]

Der Betreiber der Plattform Kino.to wurde vom LG Leipzig wegen gemeinschaftlicher unerlaubter Verwertung urheberrechtlich geschützter Werke gem. §§ 106 Abs. 1, 108a Abs. 1 UrhG verurteilt.[861] Zur Begründung führte das Gericht zunächst an, dass zwar das Setzen eines Deep-Links kein Zugänglichmachen i.S.d. § 19a UrhG darstelle, da dieser lediglich auf an anderer Stelle gespeicherte Inhalte verweise, im vorliegenden Fall seien jedoch

[857] LG Leipzig, ZUM 2013, 338.
[858] LG Leipzig, ZUM 2013, 338, 340.
[859] LG Leipzig, ZUM 2013, 338, 340.
[860] LG Leipzig, ZUM 2013, 338, 341.
[861] LG Leipzig, ZUM 2013, 338, 345.

die Urheberrechtswerke ohne den dazugehörigen Link bei dem Filehoster nicht auffindbar und damit nicht abrufbar.[862] Daher sei der Fall mit dem einer Integration in den eigenen Internetauftritt im Sinne eines zu eigen Machens der Inhalte vergleichbar.[863] Auch wenn die Links von Nutzern der Plattform hochgeladen wurden, so wurden diese vor ihrer Freischaltung durch Mitarbeiter der Plattform kontrolliert. Sodann resümiert das Gericht mit Verweis auf ein Urteil des BGH bezüglich der Zugänglichmachung von kinderpornographischen Schriften[864], dass ein öffentliches Zugänglichmachen in der Zurverfügungstellung der Plattform liege, die dem Einstellen von Dateien im Internet diene, wobei die Möglichkeit des Lesezugriffs genüge, oder im Bereitstellen entsprechender Links.[865]

b) Bewertung des Kino.to-Urteils des LG Leipzig

Auch wenn das Gericht zu einem durchaus wünschenswertem Ergebnis gelangt, so ist der Weg dorthin nicht frei von Rechtsfehlern. Zuzustimmen ist zunächst dem ursprünglichen Gedanken, dass die Inhalte ohne entsprechende Verlinkung im Internet nicht auffindbar sind. Diese Tatsache würde allerdings vielmehr hinsichtlich einer Haftung des ursprünglichen Linksetzers von Bedeutung sein, man bedenke insbesondere an den Begriff der Öffentlichkeit und des damit zusammenhängenden neuen Publikums.[866] In dem vorliegenden Fall ging es jedoch nicht um die Haftung der Linksetzer, also der Nutzer der Plattform an sich, sondern um die Haftung des Plattform-Betreibers.

Auch die vom Gericht hieraus folgende Schlussfolgerung, dass der Fall aufgrund dieser Tatsache mit einer Integration in den eigenen Internetauftritt vergleichbar sei, ist nicht ganz nachvollziehbar. Dieser Gedanke ergibt jedoch aufgrund einer anderen Tatsache Sinn, worauf das Gericht dann auch im Anschluss zusätzlich

[862] LG Leipzig, ZUM 2013, 338, 345.
[863] LG Leipzig, ZUM 2013, 338, 345.
[864] BGH BeckRS 2012, 06061.
[865] LG Leipzig, ZUM 2013, 338, 345.
[866] Siehe hierzu S. 183.

abstellt, nämlich, dass die Mitarbeiter die Plattform vor ihrer Freischaltung manuell kontrolliert haben und erst durch diese Freischaltung der Link auf die Plattform eingebunden wurde. Dies ist durchaus mit der BGH-Entscheidung in „marions-kochbuch.de“ vergleichbar, wo der Gerichtshof ein zu eigen Machen der Inhalte und entsprechend eine täterschaftliche Haftung angenommen hat. In gleicher Weise könnte der Plattformbetreiber sich also die Links seiner Nutzer zu eigen gemacht haben. Hierfür spricht nicht nur die Überprüfung der verlinkten Inhalte sondern auch die Tatsache, dass Voraussetzung für den Upload der Links war, dass das entsprechend verlinkte Filmwerk von dem Uploader in der Eingangs- und Schlusssequenz mit dem Hinweis auf Kino.to versehen wird.[867]

Unglücklicherweise geht das LG Leipzig nicht weiter auf das zu eigen Machen der Links durch den Plattformbetreiber ein, sondern folgert anschließend in lapidarer Weise, dass ein öffentliches Zugänglichmachen in der Zurverfügungstellung einer Plattform liege, die dem Einstellen von Dateien im Internet dient, wobei die Möglichkeit des Lesezugriffs genüge, oder im Bereitstellen entsprechender Links. Diese Herleitung ist jedoch problematisch. Das LG Leipzig bedient sich hier des Leitsatzes einer Entscheidung des BGH in einem strafrechtlichen Prozess hinsichtlich der Zurverfügungstellung einer Plattform mit Links auf kinderpornographische Dateien. Ob der Begriff des öffentlichen Zugänglichmachens i.S.d. § 184b StGB mit dem des § 19a UrhG identisch ist, kann zu Recht bezweifelt werden. So ist bei § 184b StGB bereits der Inhalt der Schrift an sich rechtswidrig, während § 19a UrhG lediglich das Verwertungsrecht eines an sich rechtsmäßigen Inhalts betrifft.[868] Daher ist die Übertragung der Grundsätze des Urteils des 2. Strafsenats durchaus bedenklich.

Einer solchen hätte es aber ohnehin nicht bedurft aufgrund der vom LG Leipzig zuvor gemachten Ausführungen und der bereits anerkannten Rechtsprechung im Bereich des Urheberrechts,

[867] LG Leipzig, ZUM 2013, 338, 341.
[868] So auch Reinbacher, NStZ 2014, 57, 58 f.

insbesondere dem Konstrukt des zu eigen Machens und der Kenntnis des Plattform-Betreibers von den urheberrechtsverletzenden verlinkten Inhalten.

c) Ergebnis

Sowohl der Plattformbetreiber, welcher sich die von seinen Nutzern hochgeladenen Links zu eigen macht, als auch der Linksetzende selbst können strafrechtlich im Sinne der §§ 106, 108a UrhG verantwortlich gemacht werden. Im dem Fall von Kino.to wird eine strafrechtliche Verantwortlichkeit regelmäßig gegeben sein. Denn diejenigen Nutzer, welche den Link auf der Plattform veröffentlichen, haben zuvor das entsprechende Werk auf dem Server eines Filehosters hochgeladen. Nachdem sie daraufhin von dem Filehoster den entsprechenden Link zu dem hochgeladenen Werk erhalten haben, veröffentlichen sie diesen auf der Plattform Kino.to. Während das Hochladen auf den Server des Filehosters eindeutig eine Vervielfältigungshandlung i.S.d. 16 UrhG darstellt, ist fraglich, ob hierdurch auch bereits der Tatbestand der öffentlichen Zugänglichmachung i.S.d. § 19a UrhG erfüllt ist. Denn die Datei ist grundsätzlich nur über den Link erreichbar und ohne diesen ist die Datei der Öffentlichkeit in der Regel nicht zugänglich. Erst die Veröffentlichung des Links auf der Plattform von Kino.to macht das Werk öffentlich zugänglich. Der Linksetzer wusste in der Regel von der Rechtswidrigkeit seiner Handlung und handelte somit auch in vorsätzlicher Weise.

III. Sonstige Ansprüche des Urheberrechtsinhabers gegen den ISP

Will der Urheberrechtsinhaber gegen den direkten Verletzer vorgehen, so steht er oftmals vor dem Problem, dass ihm die Identität des Rechtsverletzers nicht bekannt ist. Über entsprechende Informationen zur Identifizierung des Rechtsverletzers wird in aller Regel der ISP verfügen. Datenschutzrechtliche Vorschriften sowie die Verpflichtung zur Wahrung des Fernmeldegeheimnisses erfordern jedoch eine spezielle gesetzliche Grundlage, die es dem

ISP erlaubt, Daten zur Identifizierung ihrer Nutzer an Dritte herauszugeben.

Gem. § 101 Abs. 2 Nr. 3 UrhG, welcher Art. 8 Durchsetzungs-RL umsetzt, kann der Urheber in Fällen offensichtlicher Rechtsverletzung oder in Fällen, in denen der Verletzte gegen den Verletzer Klage erhoben hat, auch gegen eine Person, die in gewerblichem Ausmaß für rechtsverletzende Tätigkeiten genutzte Dienstleistungen erbrachte, einen Anspruch auf Auskunft geltend machen. Dieser Paragraph verschafft damit auch einen Auskunftsanspruch gegen den ISP, da dieser regelmäßig Dienstleistungen erbringt, welche der Verletzer für seine urheberrechtsverletzende Tätigkeit nutzt.

1. Offensichtliche Rechtsverletzung oder anhängiges Verfahren

Voraussetzung für einen Auskunftsanspruch gegen den ISP ist eine offensichtliche Rechtsverletzung. Die Gesetzesbegründung zu § 101 Abs. 7 UrhG, welcher ebenfalls auf Fälle offensichtlicher Rechtsverletzungen Bezug nimmt, führt aus, dass eine Rechtsverletzung offensichtlich ist, wenn die Rechtsverletzung so eindeutig ist, dass eine Fehlentscheidung oder eine andere Beurteilung im Rahmen des richterlichen Ermessens und damit eine ungerechtfertigte Belastung des zur Auskunft Verpflichteten kaum möglich ist.[869] Eine solch evidente Rechtslage wird bei Raubkopien, insbesondere sofern es sich um aktuelle Kinofilme handelt, regelmäßig gegeben sein.[870] Hingegen fehlt es an einer entsprechenden Offensichtlichkeit, wenn in tatsächlicher oder rechtlicher Hinsicht Zweifel bestehen.[871] Die Offensichtlichkeit der Rechtsverletzung soll gerade eine Ausforschung ins Blaue hinein verhindern.[872]

Im Fall von IP-Adressen ist für die Offensichtlichkeit auch von Bedeutung, dass die zur Ermittlung der IP-Adresse eingesetzte

[869] BT-Drucks. 11/4792, S. 30.
[870] Spindler in Spindler/Schuster, § 101 UrhG, Rn. 7.
[871] Bohne in Wandtke/Bullinger, § 101 Rn. 17.
[872] Dreier in Dreier/Schulze, § 101 Rn. 11.

Software zuvor validiert wurde, bspw. durch ein unabhängiges Sachverständigengutachten.[873]

Nicht erforderlich ist allerdings, dass offensichtlich ist, von welcher Person die Rechtsverletzung begangen wurde, d.h. es ist bspw. hinsichtlich der IP-Adresse unerheblich, ob bereits feststeht, dass der Inhaber der IP-Adresse die Urheberrechtsverletzung vorgenommen hat.[874]

Die zweite Alternative zur Geltendmachung des Auskunftsanspruchs, die Klageerhebung gegen den Verletzer, wird vornehmlich seine Anwendung im Offline-Bereich, bspw. hinsichtlich eines Auskunftsanspruchs über die Anzahl von urheberrechtsverletzenden Vervielfältigungsstücken gegen einen Spediteur zur Berechnung eines Schadensersatzanspruches, haben.[875] Denkbar wäre allerdings auch im Hinblick des ISP ein Auskunftsanspruch über den genauen Zeitraum der Zurverfügungstellung der rechtsverletzenden Inhalte auf der Plattform des ISP zur Berechnung des Schadensersatzanspruchs. Hinsichtlich eines Auskunftsanspruches des Urheberrechtsinhabers gegen den ISP zur Identifizierung des Rechtsverletzers hat diese zweite Alternative jedoch keine ersichtliche Relevanz, da im Zivilrecht eine Klage gegen Unbekannt nicht möglich ist.[876]

2. Gewerbliches Ausmaß

Der ISP muss seine Dienstleistungen, die zur Verletzung von Urheberrechten genutzt wurden, in gewerblichem Ausmaß erbracht haben. Ein gewerbliches Ausmaß liegt vor, wenn die Dienstleistung zur Erlangung eines unmittelbaren oder mittelbaren wirtschaftlichen oder kommerziellen Vorteils vorgenommen wird.[877]

---

[873] OLG Köln, ZUM 2012, 582; Dreier in Dreier/Schulze, § 101 Rn. 28; Bohne in Wandtke/Bullinger, § 101 Rn. 17.
[874] OLG Zweibrücken, MMR 2010, 214, 215; OLG Köln, GRUR-RR 2009, 9, 10.
[875] Bohne in Wandtke/Bullinger, § 101 Rn. 15.
[876] Bohne in Wandtke/Bullinger, § 101 Rn. 14.
[877] Reber in BeckOK UrhG, § 101, Rn. 1.

Lange Zeit umstritten war die Frage, ob auch der Rechtsverletzer in gewerblichem Ausmaß handeln muss. Diese Einschränkung wurde aus § 101 Abs. 1 UrhG hergeleitet, der ein gewerbliches Ausmaß der Rechtsverletzung voraussetzt. Der BGH hat dieser Diskussion weitgehend mit seinem Urteil „Alles kann besser werden“ ein Ende gesetzt und dem doppelten Gewerbsmäßigkeitserfordernis eine Absage erteilt.[878] Da es sich bei dem Auskunftsanspruch gegen einen Dritten um einen Hilfsanspruch zur Vorbereitung von Unterlassungsansprüchen und Schadensersatzansprüchen gegen den direkten Rechtsverletzer handelt, ist dieser nicht an die gleichen Bedingungen geknüpft wie der Auskunftsanspruch gegen den Rechtsverletzer.[879] Zudem würden von dem Auskunftsanspruch gegen Dritte vor allem Rechtsverletzungen im Internet erfasst, wo Nutzer weitgehend anonym tätig sind.[880] Bestünde der Auskunftsanspruch nur bei Rechtsverletzungen in gewerblichem Ausmaß, könne der Rechteinhaber auch Unterlassungs- und Schadensersatzansprüche nur im Falle einer Rechtsverletzung in gewerblichen Ausmaß geltend machen.[881] Dies würde dem Ziel, Rechtsverletzungen im Internet wirksam zu bekämpfen, entgegenstehen.[882]

3. Gegenstand des Auskunftsverlangens

Bei dem vom ISP begehrten Auskunftsanspruch wird es sich regelmäßig entweder um Bestandsdaten oder Nutzungs- bzw. Verkehrsdaten handeln, durch welche sich die Identität des Rechtverletzers seitens des ISP ermitteln lässt.[883]

Das es sich hier um personenbezogene Daten handelt, sind auch datenschutzrechtliche Gesichtspunkte zu beachten. Entsprechend bestimmt § 101 Abs. 9 S. 8 TMG, dass Vorschriften zum Schutz personenbezogener Daten unberührt bleiben.

---

[878] BGH GRUR 2012, 1026, 1027 f.
[879] BGH GRUR 2012, 1026, 1028.
[880] BGH GRUR 2012, 1026, 1028.
[881] BGH GRUR 2012, 1026, 1028.
[882] BGH GRUR 2012, 1026, 1028.
[883] Dreier in Dreier/Schulze, § 101 Rn. 10.

a) Bestands- und Nutzungsdaten

Die von den ISP zu beachtenden Datenschutzgrundsätze hinsichtlich der Bestands- und Nutzungsdaten vermitteln die §§ 11-15 TMG. So dürfen nach § 12 Abs. 1 TMG personenbezogene Daten zur Bereitstellung von Telemedien nur erhoben und verwendet werden, sofern das TMG oder eine andere Rechtsvorschrift, die sich ausdrücklich auf Telemedien bezieht, dies erlaubt bzw. wenn der Nutzer eingewilligt hat. Es ist grundsätzlich zwischen Bestands- und Nutzungsdaten zu unterscheiden.

Bei Bestandsdaten handelt es sich gem. § 14 Abs. 1 TMG um personenbezogene Daten eines Nutzers, die für die Begründung, inhaltliche Ausgestaltung oder Änderung eines Vertragsverhältnisses über die Nutzung von Telemedien erforderlich sind. Hierzu zählen typischerweise z.B. Name, Anschrift, E-Mail-Adresse oder aber auch eine statische IP-Adresse.[884] Diese Bestimmung ist insbesondere für den Host-Provider von Bedeutung. Da der Host-Provider nach § 13 Abs. 6 TMG seinen Nutzern, soweit technisch möglich und zumutbar, die anonyme oder pseudonymisierte Nutzung zu ermöglichen hat, ist er oftmals der einzige, dem die wahre Identität bekannt ist. Soweit vereinzelt die Auffassung vertreten wird, dass hierdurch auch gegenüber dem ISP eine solche Anonymität/Pseudonymität begründet wird[885], ist dies abzulehnen. Die Pflicht zur Gewährung von Anonymität bzw. Pseudonymität bezieht sich lediglich auf die Nutzung des Telemediums, nicht jedoch auf die Begründung eines anonymen bzw. pseudonymen Vertragsverhältnisses mit dem ISP.[886]

So kann der Host-Provider bspw. bei einem Post des Nutzers unter einem Pseudonym, diesem Pseudonym einen Namen zur Identifikation des Rechtsverletzers zuordnen.

---

[884] Spindler/Nink in Spindler/Schuster, § 14 TMG, Rn. 3.
[885] So Schnabel/Freund, CR 2010, 718, 719.
[886] Härting, NJW 2013, 2065, 2067; Spindler/Nink in Spindler/Schuster, § 13 TMG, Rn. 22.

§ 14 Abs. 2 TMG, welcher besagt, dass auf Anordnung der zuständigen Stelle, der Diensteanbieter Auskunft über die Bestandsdaten erteilen darf, soweit dies zur Durchsetzung der Rechte am geistigen Eigentum erforderlich ist, stellt selbst keine Anspruchsgrundlage für einen Auskunftsanspruch gegen den ISP dar. Hierdurch wird vielmehr klargestellt, dass der im Rahmen des Auskunftsanspruches in Anspruch Genommene den Auskunftsanspruch nicht aus datenschutzrechtlichen Gründen zurückweisen kann.[887]

Bei dem Access-Provider wird hingegen meist die IP-Adresse als Nutzungsdatum Gegenstand des Auskunftsanspruchs sein.

Gem. § 15 Abs. 1 TMG darf der ISP Nutzungsdaten nur erheben und verwenden, soweit dies erforderlich ist, um die Inanspruchnahme von Telemedien zu ermöglichen und abzurechnen. Zusätzlich wird auch der Auskunftsanspruch durch § 15 Abs. 5 S. 4 TMG legitimiert, welcher Bezug auf die entsprechende Regelung hinsichtlich der Bestandsdaten nimmt und bestimmt, dass § 14 Abs. 2 TMG entsprechend Anwendung findet. Daher darf der ISP auf Anordnung Auskunft über Nutzungsdaten zur Durchsetzung der Rechte am geistigen Eigentum geben.

Fraglich ist allerdings, ob §§ 14, 15 TMG auch eine ausreichende datenschutzrechtliche Grundlage darstellen für den direkten Auskunftsanspruch, den der Urheberrechtsinhaber gegenüber dem ISP geltend macht. Nach dem Wortlaut des § 14 Abs. 2 TMG greift die datenschutzrechtliche Erlaubnis zur Durchsetzung der Rechte am geistigen Eigentum nur bei Anordnungen einer zuständigen Stelle. Die Gesetzgebungsmaterialien führen hierzu aus, dass die Auskunft über die Daten aufgrund einer Anordnung einer öffentlichen Stelle erteilt werden darf.[888] In der datenschutzrechtlichen Begriffsbestimmung des BDSG sind öffentliche Stellen Behörden, Organe der Rechtspflege und andere öffentlich-rechtlich organisierte Einrichtungen des Bundes bzw. der

[887] Schmitz in Hoeren/Sieber/Holznagel, Teil 16.2, Rn. 224.
[888] BT-Drucks. 16/3078, S. 16.

Länder.[889] Privatpersonen oder privatrechtliche Unternehmen, welche ihre Urheberrechte durchsetzen wollen dürften nach dieser Begriffsauslegung jedenfalls nicht darunter fallen. Teilweise wird daher die Auffassung vertreten, dass eine Anordnung gem. § 14 Abs. 2 TMG nur durch öffentlich-rechtliche Rechtspersonen aufgrund einer öffentlich-rechtlichen Ermächtigungsgrundlage erlassen werden könne.[890] Eine solche Interpretation würde jedoch den § 101 Abs. 2 UrhG leerlaufen lassen. Daher ist § 14 II TMG nach seinem Zweck so auszulegen, dass er auch die Datenauskunft gem. § 101 Abs. 2 UrhG erfasst.[891]

b) Verkehrsdaten

§ 101 Abs. 9 UrhG enthält eine zusätzliche Anforderung wenn es um die Auskunft bzgl. Verkehrsdaten i.S.d. § 3 Nr. 30 TKG geht. Verkehrsdaten sind nach dieser Legaldefinition Daten, die bei der Erbringung eines Telekommunikationsdienstes erhoben, verarbeitet oder genutzt werden. Auskunft über solche Daten kann nur erteilt werden, sofern eine vorherige richterliche Anordnung über die Zulässigkeit der Verwendung der Verkehrsdaten ergangen ist. Im Rahmen der richterlichen Würdigung ist nach dem OLG Köln keine absolute Sicherheit über die tatsächlichen Vorgänge erforderlich, vielmehr reiche ein für das praktische Leben brauchbarer Grad von Gewissheit aus, der vernünftige Zweifel ausschließe.[892]

Für die Anordnung ist das Landgericht, in dessen Bezirk der zur Auskunft Verpflichtete seinen Wohnsitz, Sitz oder seine Niederlassung hat, ohne Rücksicht auf den Streitwert, zuständig. Die Kosten eines solchen Verfahrens hat der Verletzte zu tragen.

---

[889] Siehe Legaldefinition in § 2 Abs. 1 und 2 BDSG.
[890] Schmitz in Hoeren/Sieber/Holznagel, Teil 16.2, Rn. 225.
[891] So auch Ladeur, NJW 2010, 2702, allerdings im Hinblick auf das Auskunftsverfahren des § 101 Abs. 9 UrhG, wo er ausführt, dass nach den Grundsätzen der zivilrechtlichen Methodenlehre nicht nur das Gesetz entsprechend seinem Zweck ausgelegt werden muss, sondern auch nach dem Gebot der systematischen Interpretation so, dass die Rechtsvorschriften im Privatrecht so interpretiert werden, dass ein Verhältnis sinnvoller Koordination entsteht.
[892] OLG Köln, ZUM 2013, 952, 952.

Hintergrund der erforderlichen richterlichen Anordnung ist lt. § 101 Abs. 10 UrhG die Einschränkung des Fernmeldegeheimnisses.
Diese Vorschrift betrifft größtenteils den Access-Provider, da dieser den jeweiligen dynamischen IP-Adressen dem zu diesem Zeitpunkt zugewiesenen Nutzer zuordnen kann.
Insbesondere im Bereich des Peer-to-Peer-Filesharing ist eine Zuordnung der IP-Adresse oftmals die einzige Möglichkeit, um die Identität der dortigen Rechtsverletzer festzustellen.
Nicht anwendbar ist diese Bestimmung allerdings auf statische IP-Adressen, da es sich hier um Bestandsdaten und nicht um Verkehrsdaten handelt.[893]
Als problematisch für den Rechteinhaber bei der Durchführung des Auskunftsanspruches hinsichtlich der IP-Adresse könnte sich jedoch die Tatsache erweisen, dass dieser weder rechtlich verpflichtet noch dazu ermächtigt ist, diese Daten für einen längeren Zeitpunkt ohne Grund zu speichern.
Die neuen Bestimmungen der §§ 113a ff. TKG zur Vorratsdatenspeicherung, welche am 18.12.2015 durch das Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten[894] eingeführt wurden, und wonach IP-Adressen für einen Zeitraum von 10 Wochen zu speichern sind, können für einen zivilrechtlichen Anspruch nicht herangezogen werden. § 113c TKG enthält insoweit einen abschließenden Katalog hinsichtlich der Verwendung der Daten. Nicht enthalten ist die Rechtsverfolgung von Rechten des geistigen Eigentums.
Der Urheberrechtsinhaber kann allerdings auf die nach §§ 96 ff. TKG gespeicherten Verkehrsdaten zurückgreifen.[895] Danach dürfen Verkehrsdaten zum Aufbau und zur Aufrechterhaltung der Telekommunikation sowie zur Entgeltabrechnung erhoben und verwendet werden. Auch ist nach Ansicht des BGH eine Speicherung für bis zu 7 Tage im Rahmen des § 100 TKG zulässig, um Störungen an den Telekommunikationsanlagen zu erkennen,

[893] So auch Dreier in Dreier/Schulze, § 101 Rn. 35.
[894] BGBl. I S. 2218.
[895] Spindler in Spindler/Schuster, § 101 UrhG, Rn. 23.

einzugrenzen oder zu beseitigen.[896] Für eine solche Speicherung ist es nicht notwendig, dass im Einzelfall bereits Anhaltspunkte für eine Störung oder einen Fehler bestehen.[897] Eine auf 7 Tage begrenzte, anlasslose Speicherung von IP-Adressen sei deshalb grundsätzlich zulässig, sofern die Verhältnismäßigkeit gewahrt bleibe.[898] Eine Auskunft auf Grundlage dieser gespeicherten Daten kann gem. § 96 Abs. 1 S. 2 TKG erfolgen, der eine Verwendung dieser Daten zulässt, sofern dies durch die durch andere gesetzlichen Vorschriften begründeten Zwecke erforderlich ist.[899] Eine solche gesetzliche Vorschrift ist § 101 Abs. 2 Nr. 3 UrhG.

c) Abgrenzung TMG und TKG

Nach der Bestimmung des § 101 Abs. 9 UrhG, richtet sich der Richtervorbehalt lediglich auf Verkehrsdaten i.S.d. TKG, nicht jedoch auf Nutzungsdaten i.S.d. TMG. Diese unterschiedliche Behandlung scheint paradox, insbesondere vor dem Hintergrund, dass sowohl im Bereich der Verkehrsdaten als auch der Nutzungsdaten bei der Herausgabe der IP-Adresse das Fernmeldegeheimnis berührt ist. In der Praxis scheint diese Divergenz jedoch wegen der folgenden Überlegungen keine nennenswerte Rolle zu spielen.

Es ist grundsätzlich zwischen einem Access-Provider zu unterscheiden, der als Telekommunikationsanbieter klassifiziert werden kann und einem solchen der als Telemediendienstanbieter zu klassifizieren ist. Wie bereits unter B.III.4. erläutert, hängt die Einordnung von der genauen Dienstleistung ab. Handelt es sich um einen Access-Provider, dessen Tätigkeit sich darauf beschränkt, die technische Infrastruktur zur Verfügung zu stellen, ohne irgendwelche Inhalte auszusuchen oder aufzubereiten, wird dieser unter die Bestimmungen des TKG fallen.[900] Sofern der Access-Provider jedoch zusätzliche Dienste anbietet, wie bspw. eine eigene

[896] BGH MMR 2011, 341, 343 f.
[897] OLG Frankfurt, MMR 2009, 542, 544; BGH MMR 2011, 341, 343.
[898] BGH MMR 2011, 341, 344.
[899] So auch OLG Köln, MMR 2011, 759.
[900] Schmitz in Hoeren/Sieber/Holznagel, Teil 16.2, Rn. 70.

Portalseite, so besteht sein Dienst nur überwiegend in der Übertragung von Signalen über Telekommunikationsnetze und er unterliegt entsprechend den Bestimmungen des TMG.[901]

§ 11 Abs. 3 TMG bestimmt entsprechend, dass bei Telemedien, die überwiegend in der Übertragung von Signalen über Telekommunikationsnetze bestehen, für die Erhebung und Verwendung personenbezogener Daten nur § 15 Abs. 8 und § 16 Abs. 2 Nr. 4 TMG gelten. Nach der Gesetzesbegründung soll hierdurch Rechtsklarheit dahingehend verschafft werden, dass für solche Anbieter, bis auf die in § 11 Abs. 3 TMG aufgeführten Ausnahmen, lediglich die Datenschutzvorschriften des TKG anwendbar sind und dem Anbieter damit eine bessere Handhabung der Datenschutzvorschriften ermöglicht werden.[902]

In der Praxis wird daher die Großzahl der Access-Provider dieser Bestimmung und folglich den Datenschutzbestimmungen des TKG unterfallen und somit ist auch eine richterliche Anordnung hinsichtlich der Verkehrsdaten gem. § 101 Abs. 9 UrhG für den Auskunftsanspruch erforderlich.

Problematisch ist hierbei allerdings, dass, anders als § 14 und § 15 TMG, es im TKG an einer expliziten Ermächtigungsgrundlage für die Datenweitergabe zum Schutze des geistigen Eigentums fehlt.[903] § 96 Abs. 1 S. 2 TKG bestimmt jedoch, dass die Verkehrsdaten auch verwendet werden dürfen, sofern dies für durch andere gesetzliche Vorschriften begründete Zwecke erforderlich ist. Insofern kann in § 101 Abs. 9 UrhG in Verbindung mit der richterlichen Anordnung eine solche datenschutzrechtliche Grundlage gesehen werden.[904]

IV. Haftung des ISP gegenüber dem Nutzer

Sofern der ISP tätig wird, um bestimmte Inhalte zu entfernen oder zu blockieren, birgt dies grundsätzlich auch die Gefahr, dass sich

[901] Schmitz in Hoeren/Sieber/Holznagel, Teil 16.2, Rn. 70.
[902] BT-Drucks. 16/3078, S. 15 f.
[903] Czychowski/Nordemann, NJW 2008, 3095, 3097; Spindler, GRUR 2008, 574, 574.
[904] So auch Braun in BeckTKG-Kommentar, § 96 Rn. 17; Redeker, IT-Recht, Rn. 1330; Czychowski/Nordemann, NJW 2008, 3095, 3097.

ein Nutzer gegen eine Entfernung bzw. Sperrung seines Inhaltes zur Wehr setzt. Dies ist insbesondere in Fällen denkbar, in denen der Nutzer die Entfernung bzw. Sperrung für unrechtmäßig hält.
Fraglich ist, inwieweit der ISP verantwortlich ist für Inhalte, die er nach entsprechendem Hinweis entfernt bzw. blockiert, die sich allerdings im Nachhinein als nicht rechtwidrig herausstellen.

1. Vertragliche Ansprüche des Nutzers

Das Verhältnis zwischen ISP und Nutzer beruht regelmäßig auf einem Vertrag. Wie bei Internetsachverhalten üblich liegen diesem Vertragsverhältnis meist Allgemeine Geschäftsbedingungen (AGB) des ISP zugrunde.

a) Vertragliche Ansprüche gegenüber dem Host-Provider

Welche Ansprüche der Nutzer gegenüber dem Host-Provider aufgrund der Löschung oder Sperrung von rechtmäßigen Inhalten geltend machen kann, ist u.a. abhängig von der konkreten Einordnung des Vertragsverhältnisses zwischen Nutzer und Host-Provider.

aa) Vertragsrechtliche Einordnung des Hosting-Vertrags

Die vertragsrechtliche Einordnung des Vertrags zwischen Host-Provider und Nutzer ist umstritten.[905] Es handelt sich in der Regel um einen typengemischten Vertrag, der dienst-, miet- und werkvertragliche Aspekte aufweist.[906] Der BGH geht davon aus, dass sofern der Vertrag seinen Schwerpunkt in der Gewährleistung der Abrufbarkeit der Webseite des Kunden im Internet hat, es naheliegt, insgesamt einen Werkvertrag anzunehmen.[907] Allerdings dürfte der Schwerpunkt des Vertrags regelmäßig in der Vermietung, d.h. Bereitstellung und Überlassung von Speicherplatz auf der Hardware des Host-Providers liegen, so dass der Hosting-Vertrag vielmehr als Mietvertrag einzuordnen ist.[908]

[905] Ballhausen/Roggenkamp in Kilian/Heussen, Providerverträge, Rn. 26; Hoeren in Westphalen, Graf von, Vertragsrecht, E-Commerce-Verträge, Rn. 29.
[906] BGH NJW 2010, 1449, 1451.
[907] BGH NJW 2010, 1449, 1451.
[908] So auch Ballhausen/Roggenkamp in Kilian/Heussen, Providerverträge, Rn. 26 f.

bb) Ansprüche aus dem Hosting-Vertrag

Ordnet man den Hosting-Vertrag als Mietvertrag ein, besteht die Hauptleistungspflicht des Host-Providers darin, dem Nutzer Speicherplatz auf seiner Plattform bzw. seinem Server zur Verfügung zu stellen. Die Verpflichtung des Host-Providers, keine durch den Nutzer rechtmäßig eingestellten Inhalte zu löschen, lässt sich als Nebenpflicht i.S.d. § 241 Abs. 2 BGB einordnen.[909] Danach kann das Schuldverhältnis nach seinem Inhalt jeden Teil zur Rücksicht auf die Rechte, Rechtsgüter und Interessen des anderen Teils verpflichten. Durch die Entfernung bzw. Sperrung könnte in diese Rechte und Interessen des Nutzers eingegriffen werden. Als Folge könnte der Nutzer Schadensersatzansprüche nach § 280 Abs. 1 BGB gegen den Host-Provider geltend machen. Der Host-Provider hat nach § 276 BGB für fahrlässiges Handeln einzustehen. Fraglich ist, welcher Maßstab bei der Beurteilung der Fahrlässigkeit des Host-Providers im Rahmen eines durch den Urheberrechtsinhaber versendeten, unbegründeten Hinweises anzulegen ist. Missachtet der Host-Provider die im Verkehr erforderliche Sorgfalt, wenn er nach Erhalt eines konkreten Hinweises auf eine Rechtsverletzung durch den Urheberrechtsinhaber von der Korrektheit des Hinweises ausgeht und den beanstandeten Inhalt entfernt, um so auch seine Privilegierung des § 10 TMG nicht zu gefährden? Grundsätzlich ist bei einem Irrtum über die Rechtswidrigkeit die Fahrlässigkeit nicht ausgeschlossen.[910] Sofern der Schuldner nicht in der Lage ist, die rechtliche Situation selbst zu bewerten, ist er grundsätzlich dazu verpflichtet, sich Rechtsrat bei einem Rechtskundigen zu holen.[911] Auf den Host-Provider übertragen, würde dies bedeuten, dass dieser, bevor er das beanstandete Material entfernt, sich zuvor hinsichtlich dessen tatsächlicher Urheberrechtswidrigkeit vergewissern muss, ggf. unter Bezugnahme von rechtskundigen

[909] So auch im Ergebnis Ballhausen/Roggenkamp in Kilian/Heussen, Providerverträge, Rn. 37, die davon ausgehen, dass regelmäßige Datensicherungen durch den Host-Provider zu seinen Nebenpflichten gehören.
[910] Dauner-Lieb in Dauner-Lieb/Langen, § 276 Rn. 15.
[911] Grundmann in MüKo BGB, § 276 Rn. 73.

Personen, da er sonst im Innenverhältnis fahrlässig gehandelt haben könnte. Eine solch weite Auslegung könnte allerdings im Widerspruch zu den Privilegien des TMG stehen. Diese wurden vor allem konstruiert, um Rechtssicherheit für den Host-Provider zu schaffen. Allerdings stellt § 10 TMG auf die positive, d.h. tatsächliche Kenntnis des Host-Providers ab. Bei einer am Wortlaut des § 10 TMG angelehnten Interpretation ist deshalb eine Entfernung oder Sperrung des Inhaltes nicht an den Erhalt einer Mitteilung des Rechteinhabers geknüpft, sondern an die tatsächliche Kenntnis des Host-Providers. Daher könnte eine Entfernung aufgrund der Mitteilung des Rechteinhabers ohne weitergehende Prüfung als fahrlässig eingestuft werden mit der Folge, dass der Host-Provider dem Nutzer gegenüber im Innenverhältnis schadensersatzpflichtig ist.[912]

b) Vertragliche Ansprüche gegenüber dem Access-Provider

Die Ansprüche des Nutzers gegenüber dem Access-Provider richten sich nach der rechtlichen Einordnung des Vertragsverhältnisses zwischen Nutzer und Access-Provider.

aa) Vertragliche Einordnung des Access-Provider-Vertrags

Der Access-Provider-Vertrag ist regelmäßig als Dienstvertrag einzuordnen.[913] Der Access-Provider stellt dem Nutzer durch Zugang zu einem Kommunikationsnetz, bspw. dem Internet, eine Dienstleistung zur Verfügung.[914]

bb) Ansprüche aus dem Access-Provider-Vertrag

In der Verschaffung des Zugangs zu einem Kommunikationsnetz liegt die Hauptleistungspflicht des Access-Providers gegenüber seinen Kunden. Hinsichtlich der Zugangsverschaffung zum Internet trifft den Access-Provider allerdings keine vertragliche Pflicht die Abrufbarkeit aller grundsätzlich vorhandenen Angebote zu

[912] A.A Holznagel, S. 157, der bereits bei einer „plausibel erscheinenden" Verdachtsmeldung die Fahrlässigkeit des Host-Providers verneint.
[913] BGH NJW 2010, 1449, 1451; Hoeren in Westphalen, Graf von, Vertragsrecht, E-Commerce-Verträge, Rn. 9.
[914] Hoeren in Westphalen, Graf von, Vertragsrecht, E-Commerce-Verträge, Rn. 9.

gewährleisten.[915] Von daher begründet die Sperrung einzelner Webseiten oder Webseiten-Inhalte durch den Access-Provider grundsätzlich keine Pflichtverletzung gegenüber dem Nutzer, aus denen dieser Ansprüche gegen den Access Provider geltend machen könnte.

c) Ausschluss vertraglicher Ansprüche durch AGB

Der Host-Provider kann sich prinzipiell in seinen AGB gegen etwaige Ansprüche seiner Nutzer wegen Entfernung bzw. Sperrung ihrer Inhalte weitgehend absichern.[916]

Die entsprechende Klausel muss allerdings der AGB-rechtlichen Kontrolle anhand der §§ 305 ff. BGB standhalten. Ausgeschlossen dürften demnach beispielsweise Klauseln sein, welche es dem Host-Provider ermöglichen nach Belieben Inhalte seiner Nutzer zu löschen ohne sich dadurch einer Haftung gegenüber dem Nutzer auszusetzen. Ein Haftungsausschluss ist für den Bereich der Nebenpflichten zwar grundsätzlich möglich, dies allerdings gem. § 309 Nr. 7 lit. b) BGB nur für einfache Fahrlässigkeit und nicht für grobe Fahrlässigkeit oder Vorsatz. Deshalb sollte in den AGB sichergestellt werden, dass die Haftung lediglich für Fälle in denen der Host-Provider mit einfacher Fahrlässigkeit handelt, ausgeschlossen wird. Dies bedeutet, dass, sofern der Host-Provider bei der Löschung der Inhalte in guten Glauben gehandelt hat und die erforderliche Sorgfalt nicht in ungewöhnlich großem Maß verletzt hat, ein Anspruch des Nutzers gegen diesen ausgeschlossen ist.

Zudem können weitere Maßnahmen gegen den Nutzer in den AGB geregelt werden. So hat das OLG Brandenburg beispielsweise den Ausschluss und die Sperrung eines Nutzers einer Versteigerungsplattform für angemessen und damit zulässig erklärt, wenn dieser gegen die von der Plattform aufgestellten Grundsätze verstößt.[917]

---

[915] Ballhausen/Roggenkamp in Kilian/Heussen, Providerverträge, Rn. 10.
[916] Holznagel, GRUR Int. 2014, 105, 111.
[917] OLG Brandenburg, MMR 2009, 262, 262.

2. Gesetzliche Ansprüche des Nutzers

Gesetzliche Ansprüche sind sowohl durch die Kunden der Host- und Access-Provider denkbar als auch durch Nutzer, die zwar keine Kunden der Access-Provider sind, die aber von der Sperrung einer Webseite durch den Access-Provider betroffen sind.

a) Gesetzliche Ansprüche gegenüber dem Host-Provider

Denkbar wäre ein Anspruch des Nutzers gegen den Host-Provider aus § 823 Abs. 1 BGB. Danach ist derjenige, der vorsätzlich oder fahrlässig das Leben, den Körper, die Gesundheit, die Freiheit, das Eigentum oder sonstige Recht eines anderen widerrechtlich verletzt, dem anderen zum Ersatz des daraus entstandenen Schadens verpflichtet.

aa) Eigentum

Denkbar wäre zunächst eine Einordnung der elektronischen Datei als Eigentum. Das Eigentum schützt jedoch lediglich die Einwirkung auf eine Sache.[918] Sachen sind gem. § 90 BGB nur körperliche Gegenstände. Unkörperliche Gegenstände wie Software oder Dateien stellen folglich keine Sachen in diesem Sinne dar.[919] Etwas anderes gilt nur dann, wenn die Daten auf einem Datenträger, z.B. Disketten, CDs oder Festplatten, gespeichert sind.[920] Wird in diesem Fall der Datenträger geschädigt und beeinträchtigt dies die Integrität der Daten, die sich auf dem Datenträger, wie beispielsweise dem Computer des Geschädigten, befinden, so kann der Geschädigte auch eine Eigentumsverletzung gem. § 823 Abs. 1 BGB geltend machen.[921]

Befinden sich die Daten allerdings auf den Servern eines Dritten, so stellt eine Löschung dieser Daten keine Eigentumsverletzung dar.

[918] Bamberger/Roth in BeckOK BGB, § 823 Rn. 40; Wagner in MüKo BGB, § 823 Rn. 164.
[919] Wagner in MüKo, § 823 Rn. 165.
[920] BGH NJW 1993, 2436, 2438.
[921] Koch, NJW 2004, 801, 803.

bb) Sonstiges Recht

Fraglich ist, ob der Host-Provider durch die Löschung rechtmäßiger Inhalte des Nutzers ein sonstiges Recht verletzen kann.

(1) Schutz von Daten – Recht auf Integrität und Vertraulichkeit informationstechnischer Systeme

Ein Schutz von Daten als sonstiges Recht wurde bereits vereinzelt in der Literatur anerkannt[922] Die zunehmend digitalisierte Form der Datenvermittlung und die Bedeutung der Datenwirtschaft lassen in der Tat ein praktisches Bedürfnis für einen deliktischen Schutz elektronischer Daten erkennen. Dies gilt insbesondere für Daten, die nicht auf einem Datenträger des Geschädigten gespeichert sind, sondern auf fremden Servern, zu denen der Geschädigte nur einen schuldrechtlich gewährten Zugang hat.[923] Gefolgert wird dies in der neueren Literatur zumeist aus einem Urteil des BVerfG hinsichtlich heimlicher Online-Durchsuchungen.[924] Hier hat das Gericht das allgemeine Persönlichkeitsrecht, insbesondere wegen des nur lückenhaften Schutzes des Grundrechts auf informationelle Selbstbestimmung, um das Recht auf Gewährung der Vertraulichkeit und Integrität informationstechnischer Systeme (sog. Computer-Grundrecht) erweitert.[925] Nach den Ausführungen des BVerfG ist das Computer-Grundrecht anzuwenden, wenn in IT-Systeme eingegriffen wird, die allein oder in ihren technischen Vernetzungen personenbezogene Daten in einem Umfang und in einer Vielfalt enthalten können, dass ein Zugriff auf dieses System es ermöglicht, einen Einblick in wesentliche Teile der Lebensgestaltung einer Person zu gewinnen oder gar ein aussagekräftiges Bild der Persönlichkeit zu erhalten.[926] Insofern ist auch die Integrität von IT-Systemen betroffen, sobald in einer Weise auf das System zugegriffen wird, dass dessen Leistungen,

[922] Spindler in BeckOK BGB 2015, § 823 Rn. 93; Faustmann, VuR 2006, 260, 263; Meier/Wehlau, NJW 1998, 1585; 1588; Zech, GRUR 2015, 1151, 1158.
[923] Spindler in BeckOK BGB 2015, § 823 Rn. 93.
[924] BVerfG MMR 2008, 315.
[925] BVerfG MMR 2008, 315, 317 ff.
[926] BVerfG MMR 2008, 315, 318.

Funktionen und Speicherinhalte durch einen Dritten genutzt werden können.[927] Denn dann sei die entscheidende technische Hürde für eine Ausspähung, Überwachung oder Manipulation des Systems genommen.[928]

Auch wenn das Urteil in erster Linie Wirkung hinsichtlich staatlicher Eingriffe entfaltet, wird teilweise vertreten, dass durch die Aufzeigung der Bedeutung und Gefährdung der Datenverarbeitung eine Prüfung zivilrechtlicher Konsequenzen geboten sei.[929] *Bartsch* führt diesbezüglich aus, dass die Integrität bei einer Manipulation des Systems betroffen sei, welche auch das Löschen von Daten beinhalte.[930] Es wäre nach dieser Argumentation folglich ein Eingriff in ein sonstiges Recht in Form des Rechts auf Integrität und Vertraulichkeit informationstechnischer Systeme möglich. Allerdings handelt es sich insoweit nur um ein Auffangrecht, weshalb eine sorgsame Interessenabwägung geboten ist.[931]

Wagner hingegen hält eine Einordnung des Datenbestandes als sonstiges Recht ohne weitergehende Ausführungen für nicht praktikabel, da sich dies inhaltlich nicht fixieren und in seinem Schutzbereich definieren ließe.[932]

(2) Eingerichteter und ausgeübter Gewerbebetrieb

Handelt es sich bei dem Nutzer um einen Unternehmer, wäre zudem ein Eingriff in den eingerichteten und ausgeübten Gewerbebetrieb denkbar. Das Recht am eingerichteten und ausgeübten Gewerbebetrieb wurde von der Rechtsprechung als Auffangtatbestand entwickelt und umfasst das Unternehmen in seiner Gesamtheit, insbesondere den Tätigkeitskreis, die Geschäftsverbindungen, den Kundenstamm, die Kommunikationsbeziehungen des Unternehmens sowie generell die ungestörte Fortsetzung der bisherigen Tätigkeit aufgrund der

[927] BVerfG MMR 2008, 315, 318.
[928] BVerfG MMR 2008, 315, 318.
[929] Bartsch, CR 2008, 613, 613; Spindler in BeckOK BGB 2015, § 823 Rn. 93.
[930] Bartsch, CR 2008, 613, 615.
[931] Bartsch, CR 2008, 613, 616; Spindler in BeckOK BGB 2015, § 823 Rn. 93.
[932] Wagner in MüKo BGB, § 823 Rn. 165.

bereits getroffenen Vorkehrungen.[933] Wegen dieses umfassenden Anwendungskreises hat die Rechtsprechung schon früh eine Betriebsbezogenheit des Eingriffs gefordert, d.h. dass der Eingriff irgendwie gegen den Betrieb als solchen gerichtet ist.[934] Einer Betriebsbezogenheit steht es jedoch nicht entgegen, wenn nur einzelne Geschäftsaktivitäten des Unternehmens betroffen sind.[935] Vielmehr soll hierdurch sichergestellt werden, dass bloß mittelbare Eingriffe, die vom Unternehmen ablösbare Rechtsgüter betreffen, nicht in den Schutzbereich fallen.[936]

Ein Eingriff in den eingerichteten und ausgeübten Gewerbebetrieb wurde von der Rechtsprechung bspw. bejaht für die ungerechtfertigte Zusendung vorgerichtlicher Abmahnungen aus Schutzrechten.[937] Auch die Entfernung bzw. Löschung einzelner Inhalte könnte einen solchen Eingriff darstellen. Es wird bei der Beurteilung jedoch auf den jeweiligen Eingriff sowie dessen Intensität ankommen. Das Recht am eingerichteten und ausgeübten Gewerbebetrieb ist ein sog. offener Tatbestand, dessen genauer Inhalt und Grenzen sich erst aus einer Abwägung der im konkreten Fall kollidierenden Interessen ergeben.[938]

Grundsätzlich ist eine Einordnung als Eingriff in den eingerichteten und ausgeübten Gewerbebetrieb denkbar.

cc) Rechtswidrigkeit

Die Tatsache, dass nach dem Wortlaut des § 823 Abs. 1 BGB sich die Rechtswidrigkeit nicht auf das Verhalten des Schädigers sondern auf die Verletzung der dort genannten Rechtsgüter bezieht, hat Rechtsprechung und Literatur in zwei Lager gespalten, die entweder der Lehre vom Erfolgsunrecht oder der Lehre vom Handlungsunrecht folgen.[939] Nach der Erfolgsunrechtslehre indiziert die Verletzung regelmäßig bereits die Rechtswidrigkeit

[933] Spindler in BeckOK BGB 2015, § 823 Rn. 105.
[934] BGH NJW 1959, 479, 481.
[935] Wagner in MüKo BGB, § 823 Rn. 257.
[936] Spindler in BeckOK BGB 2015, § 823 Rn. 108; Wagner in MüKo BGB, § 823 Rn. 257.
[937] Förster in BeckOK BGB 2016, § 823 Rn. 197.
[938] Förster in BeckOK BGB 2016, § 823 Rn. 188 m.w.N.
[939] Wagner in MüKo BGB, § 823 Rn. 4.

wohingegen die Lehre vom Handlungsunrecht einen Rückschluss vom Erfolg auf die Rechtswidrigkeit ablehnt und stattdessen auf die Rechtswidrigkeit der Handlung abstellt.[940]

Die heute h.M. differenziert zwischen unmittelbaren und mittelbaren Eingriffen in die Rechtsgüter und bestimmt entsprechend, dass unmittelbare Rechtsverletzungen ohne Weiteres rechtswidrig sind, sofern keine Rechtfertigungsgründe greifen, während es für einen mittelbar wirkenden Eingriff einer Verletzung der Sorgfaltspflicht bedarf.[941]

Grundsätzlich indiziert die Erfüllung der Tatbestandsvoraussetzungen die Rechtswidrigkeit.[942] Etwas anderes gilt jedoch bei den sog. Rahmenrechten, also den nicht namentlich benannten Schutzgütern des § 823 Abs. 1 BGB.[943] Bei diesen Rahmenrechten ist die Rechtswidrigkeit positiv auf Grundlage einer umfassenden Güter- und Pflichtenabwägung festzustellen.[944] Von maßgeblicher Bedeutung ist hierbei die Zweckrichtung und Berechtigung des Eingriffes sowie die Art des Schutzbereiches in den eingegriffen wird, unter Beachtung der Verhältnismäßigkeit.[945] Ein Eingriff in das Rahmenrecht ist rechtswidrig, wenn das Schutzinteresse des Betroffenen die schutzwürdigen Interessen der anderen Seite überwiegt.[946]

Die Interessen des Host-Providers betreffen seinen eingerichteten und ausgeübten Gewerbebetrieb, den er vor Ansprüchen der Rechteinhaber schützen will. Aus diesem Grund liegt es in seinem Interesse einer Aufforderung zur Löschung bestimmter Inhalte durch den Rechteinhaber umgehend Folge zu leisten. Durch Löschung der beanstandeten Inhalte kann er gegen ihn gerichtete Unterlassungsanordnungen sowie spätere darauf basierende etwaige Ordnungsgelder bzw. eine Ordnungshaft verhindern. Auf

[940] Spindler in BeckOK BGB 2015, § 823 Rn. 9.
[941] Spindler in BeckOK BGB 2015, § 823 Rn. 10; Wagner in MüKo BGB, § 823 Rn. 7.
[942] Förster in BeckOK BGB 2016, § 823 Rn. 259.
[943] Förster in BeckOK BGB 2016, § 823 Rn. 259.
[944] Mann in Spindler/Schuster, § 823 Rn. 60.
[945] Bamberger in BeckOK BGB, § 12 Rn. 169.
[946] Bamberger in BeckOK BGB, § 12 Rn. 169.

der anderen Seite beeinträchtigt eine Löschung bzw. Sperrung von rechtmäßigen Inhalten die Interessen des Inhalteanbieters. Betroffen sein könnte das Recht am Datenbestand sowie das Recht am eingerichteten und ausgeübten Gewerbebetrieb. Zur Beurteilung der Rechtswidrigkeit kommt es auf die spezifischen Umstände des Einzelfalls an. Es ist durchaus denkbar, dass die Interessen des Host-Providers gegenüber denen des Inhalteanbieters überwiegen und der Eingriff daher nicht als rechtswidrig eingeordnet wird.

dd) Schuldhafte Verletzung

Für die deliktische Haftung des Host-Providers bedarf es zudem einer fahrlässigen oder vorsätzlichen Handlung.

Löscht der Host-Provider bestimmte Inhalte aufgrund einer Mitteilung eines Dritten, ist zu untersuchen, ob der Host-Provider erkennen konnte, dass es sich um eine fehlerhafte Mitteilung handelte und somit eine Verletzung der sonstigen Rechte des Nutzers vermeiden konnte. Da die Löschung von Inhalten nach § 10 TMG positive Kenntnis voraussetzt, ist im Zweifel fahrlässiges Handeln seitens des Host-Providers anzunehmen, wenn er bei der Prüfung der behaupteten Rechtsverletzung die im Verkehr erforderliche Sorgfalt außer Acht gelassen hat und es infolge dessen zu der Löschung von rechtsmäßigen Inhalten kam.[947]

b) Gesetzliche Ansprüche gegenüber dem Access-Provider

Bei der Geltendmachung von Ansprüchen gegenüber dem Access-Provider kann zwischen folgenden zwei Szenarien unterschieden werden: der Haftung gegenüber Nutzern, die aufgrund der Sperrung von Inhalten keinen Zugang mehr zu diesen Inhalten haben sowie die Haftung gegenüber den Nutzern bzw. Webseitenbetreibern, deren Inhalte von dem Access-Provider gesperrt wurden.

[947] Siehe zum Verschulden des Host-Providers S. 214.

aa) Haftung wegen Sperrung des Zugangs zu Informationen

Sperrt der Access-Provider einzelne Webseiten, tangiert dies den Informationszugang des Nutzers und damit die Informationsfreiheit des Art. 5 Abs. 1 GG.

Ansprüche aus § 823 Abs. 1 BGB könnte der Nutzer allerdings lediglich geltend machen, sofern die Informationsfreiheit sich als sonstiges Recht einordnen ließe. Als sonstige Rechte sind nur absolute Rechte anerkannt, also ausschließliche Rechte die gegenüber jedermann wirken.[948] Hierunter fallen auch die durch die Rechtsprechung entwickelten Rahmenrechte des Allgemeinen Persönlichkeitsrechts, welches aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG hergeleitet, sowie des Rechts am eingerichteten und ausgeübten Gewerbebetrieb, welches aus Art. 14 GG hergeleitet wird.[949]

Art. 5 GG gewährt jedem das Recht sich aus allgemein zugänglichen Quellen zu unterrichten. Als allgemein zugängliche Quellen können solche angesehen werden, die dazu geeignet und bestimmt sind, einem nicht bestimmbaren Personenkreis Informationen zu verschaffen.[950] Geschützt ist sowohl die Entgegennahme von Informationen als auch die aktive Informationsbeschaffung.[951] In erster Linie handelt es sich bei der Informationsfreiheit um ein Abwehrrecht gegen jedwede staatliche Maßnahme, die eine Verhinderung der Rezeption gewünschter Informationen darstellt.[952] Sie verfügen allerdings auch über einen objektiven Grundrechtsgehalt und strahlen ins Privatrecht aus, wo sie unmittelbare Drittwirkung gegenüber anderen Grundrechtsträgern entfalten.[953]

[948] Spindler in BeckOK 2015, § 823 BGB Rn. 72.
[949] Spindler in BeckOK 2015, § 823 BGB Rn. 72.
[950] BVerfG NJW 1970, 235, 237.
[951] BVerfG NJW 1970, 235, 236 f.
[952] Fink in Spindler/Schuster, C. Verfassungsrecht, Rn. 22.
[953] Fink in Spindler/Schuster, C. Verfassungsrecht, Rn. 27.

Es handelt sich folglich bei dem Recht auf Informationsfreiheit schon nicht um ein absolutes Recht, welches durch Zuweisungsgehalt[954] und Ausschlussfunktion[955] geprägt wird.

Zudem kann aus Art. 5 Abs. 1 GG kein genereller Anspruch auf Erschließung jeder gewünschten Informationsquelle abgeleitet werden.[956]

Auch eine Haftung nach § 823 Abs. 2 BGB, wonach den Schädiger eine Schadensersatzpflicht trifft, sofern dieser gegen ein den Schutz eines anderen bezweckendes Gesetz verstößt, ist vorliegend nicht gegeben. Zwar handelt es sich bei den Normen des Grundgesetzes um ein materielles Gesetz, welches grundsätzlich in den Anwendungsbereich des § 823 Abs. 2 BGB fällt, diese beschränken sich jedoch regelmäßig auf generalklauselartige Garantien.[957] Eine Anwendbarkeit dieser Normen im Rahmen des § 823 Abs. 2 BGB setzt hingegen voraus, dass diese durch das BVerfG konkretisiert wurden und entsprechend konkrete Verhaltenspflichten statuieren, die dem Individualschutz im Verhältnis zwischen Privatpersonen dienen.[958]

Eine gesetzliche Haftungsgrundlage des Nutzers gegen den Access-Provider wegen Sperrung einzelner Webseiten ist daher nicht ersichtlich.

bb) Haftung wegen Sperrung eigener Inhalte durch Access-Provider

Der Access-Provider könnte jedoch demjenigen Nutzer bzw. Webseitenbetreiber gegenüber verantwortlich sein, dessen Webseiten er sperrt.

---

[954] Die Zuweisungstheorie fragt danach, ob der dem Empfänger zugeflossene Vorteil von der Rechtsordnung dem Gläubiger zugewiesen ist und deshalb im Ergebnis auf seine Kosten ging, siehe Schwab in MüKo BGB, § 812 Rn. 244.

[955] Die Ausschlussfunktion bezeichnet das gegenüber jedermann bestehende Eingriffsverbot, siehe Wagner in Müko BGB, § 823 Rn. 205.

[956] Fink in Spindler/Schuster, C. Verfassungsrecht, Rn. 24.

[957] Wagner in MüKo BGB, § 823 Rn. 394.

[958] Wagner in MüKo BGB, § 823 Rn. 394; a.A. Spindler in BeckOK BGB 2015, § 823 Rn. 147, der die Normen des Grundgesetzes grundsätzlich aufgrund der fehlenden Addressierung an Privatpersonen nicht zu den Schutzgesetzen zählen, mit Ausnahme von Grundgesetznormen, die nach Wortlaut und Systematik an Privatpersonen gerichtet sind (z.B. Art. 48 Abs. 2 GG, Art. 9 Abs. 3 GG).

(1) Eingerichteter und ausgeübter Gewerbebetrieb

Die Sperrung einer kommerziellen Webseite könnte einen Eingriff in den eingerichteten und ausgeübten Gewerbebetrieb des Unternehmers darstellen.[959]

Sperrt beispielsweise der Access-Provider die Webseite einer Video-Plattform, da er der Auffassung ist, auf dieser befänden sich größtenteils urheberrechtsverletzende Inhalte, so trifft dies unmittelbar das Geschäftsmodell und somit den Gewerbebetrieb des Webseiten-Betreibers. Obwohl die Sperre dazu gedacht ist, lediglich unrechtsmäßige Inhalte zu sperren, so trifft der Eingriff unter Umständen auch dort vorhandene rechtsmäßige Inhalte. Da die Sperre gerade darauf gerichtet, dass die Webseite nicht mehr für die Nutzer des Access-Providers erreichbar ist, kann nach der hier vertretenen Auffassung eine Zielgerichtetheit angenommen werden.[960]

(2) Recht auf Integrität und Vertraulichkeit informationstechnischer Systeme

Fraglich ist, ob bei der Sperrung von privaten Webseiten das Recht auf Integrität und Vertraulichkeit informationstechnischer Systeme als sonstiges Recht des Webseitenbetreibers verletzt sein kann.

Vorliegend könnte durch die Sperrung der Webseite das Recht auf Integrität des Systems betroffen sein. *Bartsch* führt aus, dass auch bei dem Sperren des Zugangs zu Daten, Netzen und Diensten, ein Verstoß gegen die Integrität vorliegen kann.[961] Dies gelte auch wenn, wie beim Sperren bspw. einer bestimmten Webseite, das System an sich weitgehend unbeeinträchtigt bliebe.[962] Eine Verletzung des Rechts auf Integrität und Vertraulichkeit informationstechnischer Systeme könnte durch die Sperrung einzelner Webseiten durch den Access-Provider folglich gegeben sein. Die Sperre bewirkt, dass die dort vorhandenen Daten für die

[959] So auch Spindler, GRUR 2014, 826, 833, allerdings ohne weitere Begründung.
[960] Zweifelnd hinsichtlich des zielgerichteten Eingriffs bei Kollateralschäden: Spindler, GRUR 2014, 826, 833.
[961] Bartsch, CR 2008, 613, 615.
[962] Bartsch, CR 2008, 613, 615.

Nutzer des Access-Providers nicht mehr erreichbar sind. Geht man davon aus, dass auch der Zugang zu Daten durch das Recht auf Integrität und Vertraulichkeit informationstechnischer Systeme geschützt ist, könnte die Sperre durch den Access-Provider einen Eingriff in dieses Recht darstellen. Allerdings wird es hier im Rahmen einer Interessenabwägung auch auf die Erheblichkeit des Eingriffes ankommen.[963]

(3) Urheberrecht

Eine Webseite kann aufgrund ihrer schöpferischen Gestaltung Urheberrechtsschutz bspw. als Sprachwerk, Werk der angewandten Kunst oder als Darstellung wissenschaftlicher oder technischer Art beanspruchen.[964] Fraglich ist jedoch, ob die Sperrung eines urheberrechtlich geschützten Werkes den Urheber in seinen Urheberrechten verletzt. Dies ist zu verneinen. Durch die Sperrung des Zugangs zu einer Webseite wird diese weder bearbeitet noch entstellt. Die Integrität der Webseite wird nicht tangiert. Auch ein Eingriff in die Ausschließlichkeitsrechte des Urhebers wird hierdurch nicht berührt.

Ein Anspruch aufgrund einer Verletzung der Urheberrechte des Webseitenbetreibers ist folglich bei einer Zugangssperrung dieser Webseite nicht gegeben.

(4) Rechtswidrigkeit

Bei den hier einschlägigen Rahmenrechten wird die Rechtswidrigkeit nicht bereits durch die Rechtsgutverletzung indiziert.[965] Die Rechtswidrigkeit ist vielmehr positiv aufgrund einer umfassenden Güter- und Pflichtenabwägung festzustellen.[966] Auf der einen Seite stehen im vorliegenden Fall die Interessen des Access-Providers und seinem eingerichteten und ausgeübten Gewerbebetrieb. Kommt er der Mitteilung des Rechteinhabers über eine Rechtsverletzung nicht nach, droht im eine durch ein Gericht

[963] Bartsch, CR 2008, 613, 616.
[964] Koch in Hoeren/Sieber/Holznagel, Teil 26.1 Rn. 102.
[965] BeckOK BGB 2016, § 823 Rn. 259.
[966] Mann in Spindler/Schuster, § 823 Rn. 60.

erlassene Unterlassungsverpflichtung, kommt er dieser Unterlassungsverpflichtung nicht nach, so treffen ihn empfindliche Ordnungsgelder bzw. ersatzweise Ordnungshaft. Auf der anderen Seite kann die Sperrung einer Webseite einen Eingriff in den eingerichteten und ausgeübten Gewerbebetrieb bzw. das Recht auf Integrität und Vertraulichkeit informationstechnischer Systeme darstellen. Es wird im Rahmen dieser Interessenabwägung auf die konkreten Umstände des Einzelfalls ankommen. Aufgrund der weitreichenden Folgen für den Access-Provider, falls er einer Sperrungsanordnung nicht nachkommt, wäre es jedoch nach der hier vertretenen Ansicht denkbar, im Einzelfall eine Rechtswidrigkeit zu verneinen.

(5) Verschulden

Auch bei der Sperrung einer Webseite hängt ein Verschulden des Access-Providers davon ab, ob er bei der Sperrung der Webseite Sorgfaltspflichten außer Acht gelassen hat. Dies bedeutet, dass der Access-Provider nach Mitteilung über behauptete Rechtsverletzungen grundsätzlich dazu angehalten ist, diese Behauptung zu überprüfen und nicht blind auf Zuruf zu sperren.

c) Gesetzliche Ansprüche gegen den Cache-Provider

Gesetzliche Ansprüche desjenigen, dessen Inhalte von dem Cache-Provider gelöscht wurden, sind nicht ersichtlich. Der Cache-Provider löscht die Inhalte lediglich aus seinem Zwischenspeicher, es besteht kein grundsätzlicher Anspruch des Inhalteanbieters darauf, dass der Cache-Provider seine Inhalte zur schnelleren Übermittlung für einen bestimmten Zeitraum zwischenspeichert.

d) Gesetzliche Ansprüche gegen den Suchmaschinenanbieter

Da sowohl zwischen dem Nutzer einer Suchmaschine und dem Suchmaschinenanbieter als auch zwischen dem von der Entfernung eines Links Betroffenen und dem Suchmaschinenanbieter kein vertragliches Verhältnis besteht, kommen hier lediglich gesetzliche Ansprüche in Frage.

Es besteht jedoch weder ein Anspruch zur Aufnahme in die Ergebnisliste eines Suchmaschinenanbieters noch ein Anspruch darauf, sämtliche Inhalte des Internets in der Ergebnisliste eines Suchmaschinenanbieters angezeigt zu bekommen. Zudem ist der Inhalt, der aus der Ergebnisliste des Suchmaschinenanbieters gelöscht wurde, noch weiterhin an seinem Ursprungsort auffindbar. Gesetzliche Ansprüche des Nutzers einer Suchmaschine oder des durch die Entfernung des Links aus den Ergebnislisten des Suchmaschinenanbieters Betroffenen sind daher nicht ersichtlich.

3. Ergebnis

Eine Geltendmachung von Schadensersatzansprüchen aufgrund der Löschung bzw. Sperrung von Inhalten durch Host- und Access-Provider ist nur bedingt Erfolg versprechend. Während der Nutzer unter bestimmten Voraussetzungen sowohl einen Anspruch aus Vertrag als auch aus Gesetz gegen den Host-Provider herleiten kann, wird der Nutzer einen Anspruch gegen den Access-Provider lediglich auf gesetzliche Ansprüche stützen können.

Bislang gibt es hierzu keine einschlägige Rechtsprechung. Neben den rechtlichen Hürden sowie der Schwierigkeit der Bestimmung des konkreten Schadens wird die Geltendmachung von Ansprüchen in der Praxis vor allem daran scheitern, dass der Nutzer wegen der schwer zu prognostizierenden Erfolgsaussichten davor zurückschrecken wird, gerichtlich gegen den Host- oder Access-Provider vorzugehen.

V. Selbstregulatorische Maßnahmen der ISP

Im Januar hat die Kölner Forschungsstelle für Medienrecht eine im Auftrag des Bundesministeriums für Wirtschaft und Technologie vergleichende Studie über Modelle zur Versendung von Warnhinweisen durch Access-Provider bei Urheberrechtsverletzungen an Nutzer vorgelegt.[967] Hintergrund hierfür war das im Koalitionsvertrag der 17. Legislaturperiode

[967]Schwartmann, Vergleichende Studie über Modelle zur Versendung von Warnhinweisen.

festgeschriebene Ziel *„bessere und wirksame Instrumente zur konsequenten Bekämpfung von Urheberrechtsverletzungen im Internet [zu, Anmerkung des Verfassers] schaffen“*.[968] Dazu sollten auch Möglichkeiten der Selbstregulierung unter Beteiligung von Rechteinhabern und Serviceprovidern gefördert werden.[969] Initiativen für gesetzliche Internetsperren bei Urheberrechtsverletzungen wurden hingegen explizit abgelehnt.[970]

Im Ergebnis schlägt die Studie ein sog. vorgerichtliches Mitwirkungsmodell vor, welches zunächst nur auf aufklärende und warnende Hinweise setzt und erst nach der dritten Warnung Sanktionen gegen den Nutzer vorsieht.[971] Demnach soll der Rechteinhaber bei Feststellung eines Rechtsverstoßes durch eine bestimmte IP-Adresse, den betroffenen Zugangsanbieter hierüber informieren, welcher wiederum eine aufklärende Warnung an den IP-Adressen-Inhaber sendet sowie eine anonymisierte Verstoßliste hinsichtlich des Anschlussinhabers anlegt.[972] Nach dem dritten Verstoß soll diese Liste in anonymisierter Form an den Rechteinhaber geleitet werden, welcher dann im Wege eines gerichtlichen Auskunftsverlangens Name und Anschrift des Anschlussinhabers heraus verlangen kann.[973]

Der eco-Verband hat diese Studie zum Anlass genommen, seinerseits ein Kurzgutachten in Auftrag gegeben, um sich mit dem Vorschlag dieser Studie auseinanderzusetzen.[974] *Hoeren* wirft in dem Kurzgutachten eine Reihe von Bedenken gegen das in der Studie als zulässig und im Einklang mit geltendem Recht vorgeschlagene vorgerichtliche Mitwirkungsmodell auf. Er sieht hier insbesondere eine Privatisierung der Rechtsdurchsetzung, bei

---

[968] Koalitionsvertrag von CDU, CSU und FDP, S. 103.
[969] Koalitionsvertrag von CDU, CSU und FPD, S. 103.
[970] Koalitionsvertrag von CDU, CSU und FDP, S. 103 f.
[971] Schwartmann, Vergleichende Studie über Modelle zur Versendung von Warnhinweisen, S. 338.
[972] Schwartmann, Vergleichende Studie über Modelle zur Versendung von Warnhinweisen, S. 337.
[973] Schwartmann, Vergleichende Studie über Modelle zur Versendung von Warnhinweisen, S. 337.
[974] Hoeren, Kurzgutachten zur BMWi-Studie.

der es an einem Richtervorbehalt i.S.d. § 101 Abs. 9 UrhG fehlt.[975] Dem Nutzer würde es an einem außergerichtlichen Instrumentarium fehlen, um sich gegen unberechtigte Vorwürfe zu wehren, was im Hinblick auf die verfassungsrechtlich gewährleistete Unschuldsvermutung[976] äußerst bedenklich sei.[977] Zudem würde ein solches Warnhinweismodell einen ungerechtfertigten Eingriff besonderer Intensität in die Privatautonomie darstellen[978] sowie gegen die grundgesetzlich gewährleistete Berufsausübungsfreiheit, Art. 12 Abs. 1 GG, und Eigentumsgarantie, Art. 14 GG, der Access-Provider verstoßen[979]. Dem Access-Provider würde ein hoher Aufwand an Personal- und Sachkosten entstehen, obwohl dem Access-Provider die Urheberrechtsverletzungen an sich nicht zurechenbar seien.[980] Zu guter Letzt verstoße das Modell gegen das Fernmeldegeheimnis und sei aus datenschutzrechtlicher Sicht äußerst bedenklich.[981] So fehle es bereits an einer gesetzlichen Grundlage für die Verwendung der Daten, eine solche ergebe sich auch nicht aus dem TKG.[982] Zudem stelle auch die anonymisierte Verstoßliste ein personenbezogenes Datum dar.[983] Es handele sich hierbei um keine Anonymisierung i.S.d. Datenschutzrechtes, da ein Personenbezug ohne Weiteres möglich und sogar gewollt sei.[984]

Zu einer Umsetzung eines entsprechenden Modells ist es nie gekommen. So hat u.a. die damalige Justizministerin dem Modell eine klare Absage erteilt.[985]

---

[975] Hoeren, Kurzgutachten zur BMWi-Studie, S. 10.
[976] An einer expliziten Festschreibung der Unschuldsvermutung im deutschen Recht fehlt es, sie ist allerdings zwingende Folge des Rechtsstaatsprinzips sowie kraft Art. 6 Abs. 2 der Europäischen Menschenrechtskonvention Bestandteil des positiven Rechts der Bundesrepublik Deutschland im Range eines Bundesgesetzes, siehe auch BVerfG NJW 1990, 2741.
[977] Hoeren, Kurzgutachten zur BMWi-Studie, S. 11.
[978] Hoeren, Kurzgutachten zur BMWi-Studie, S. 13 ff.
[979] Hoeren, Kurzgutachten zur BMWi-Studie, S. 22 ff.
[980] Hoeren, Kurzgutachten zur BMWi-Studie, S. 27.
[981] Hoeren, Kurzgutachten zur BMWi-Studie, S. 29 ff.
[982] Hoeren, Kurzgutachten zur BMWi-Studie, S. 30.
[983] Hoeren, Kurzgutachten zur BMWi-Studie, S. 33.
[984] Hoeren, Kurzgutachten zur BMWi-Studie, S. 32.
[985] Briegleb: Justizministerin: Three Strikes „mit mir nicht".

VI. Zusammenfassung

Die Privilegien der §§ 7-10 TMG haben in Deutschland in ihrer derzeitigen Auslegung so gut wie keine nennenswerte Bedeutung. In sämtlichen Bereichen erschuf die Rechtsprechung ein System, welches die Bestimmungen zur Haftungsfreistellung der ISP vernachlässigt bzw. für die Auferlegung von Pflichten seitens des ISP, wie bspw. der Verpflichtung zur Entfernung oder Sperrung, nutzt. Einzig § 7 Abs. 1 S. 1 TMG wird von der Rechtsprechung herangezogen, wenn der Umfang und das Ausmaß etwaiger Verpflichtungen des ISP behandelt werden.

Die Verantwortlichkeit der ISP bestimmt sich daher weitgehend nach den allgemeinen Grundsätzen. Dies gilt auch für eine etwaige Inanspruchnahme der Provider durch betroffene Internetnutzer.

Von dem erklärten Ziel der Privilegien, der Schaffung von Rechtssicherheit auf Seiten der ISP, kann daher keine Rede sein. Vielmehr sehen sich die ISP mit einer ständig erweiterten Rechtsprechung konfrontiert, die versucht durch eine einzelfallabhängige Interessenabwägung die widerstreitenden Grundrechtspositionen ins Gleichgewicht zu bringen, oft zum Nachteil des ISP.

D. Verantwortlichkeit und Privilegien der ISP in den USA

Auch in den USA ist die Providerhaftung Gegenstand einer stetigen Debatte. Während das kodifizierte Recht hinsichtlich der Privilegierung von ISP in vielen Punkten dem deutschen Recht sehr ähnlich ist, gibt es doch teils erhebliche Unterschiede in der Anwendung dieser Rechtsvorschriften sowie in den politischen und den privatrechtlichen Bemühungen, die ISP stärker in den „Kampf gegen Cyberkriminalität“ einzubinden.

I. Einführung in das U.S.-amerikanische Recht

Zum besseren Verständnis für die in diesem Kapitel folgenden Ausführungen, wird zunächst in der gebotenen Kürze das Rechtssystem der USA vorgestellt. Augrund seiner angelsächsischen Wurzeln unterscheidet sich das U.S.-

amerikanische Recht, welches auf dem Common Law-System basiert, insbesondere im Hinblick auf die Rechtssetzung in einigen Aspekten erheblich vom kontinental-europäischen *Civil Law* System.

1. Rechtsquellen

Die Rechtsquellen des U.S.-amerikanischen Rechts können grundsätzlich unterteilt werden in *primary authority* (*hard law*) und *secondary authority* (*soft law*).[986]

Zu den Quellen der *primary authority* gehören das sog. *case law* sowie das kodifizierte Recht, die *secondary authority* umfasst sog. *Restatements of Law*[987], Fachaufsätze (*law review articles)* sowie Fachbücher oder andere Kommentare.[988]

a) Richterrecht - Case Law

Die Essenz des *common law* liegt darin, dass es auf früheren Gerichtsentscheidungen aufgebaut ist, sog. *precedents*.[989] Die *precedents* entfalten eine Bindungswirkung für darauffolgende Entscheidungen höherer Gerichte (*doctrine of stare decisis*), allerdings lediglich im Hinblick auf die tragenden Urteilsgründe (*ratio decidendi*) und nicht bloßer *obiter dicta*.[990]

b) Kodifiziertes Recht - Statutes

Die wichtigste Rechtsquelle neben dem *case law* ist das kodifizierte Recht (*statutes*). Insbesondere seit Ende des 19ten Jahrhunderts hat es immer mehr an Bedeutung gewonnen, so dass heute das geschriebene Recht eher die Regel als die Ausnahme ist.[991]

---

[986] Reiley/de la Vega, S. 37.
[987] *Restatements of Law* werden herausgegeben von dem American Law Institute (https://www.ali.org). Sie behandeln die in verschiedenen Rechtsgebieten durch die Rechtsprechung herausgearbeiteten Prinzipien des *common law* und bereiten diese versehen mit zusätzlichen Ausführungen und Kommentaren systematisch auf.
[988] Reiley/de la Vega, S. 37.
[989] Burnham, Introduction to U.S. Law, S. 44.
[990] Hay, Law of the U.S., Rn. 22.
[991] Hay, Law of the U.S., Rn. 17; Burnham, Introduction to U.S. Law, S. 50.

Gesetze existieren sowohl auf Bundesebene (*federal statutes*[992]) als auch auf bundesstaatlicher Ebene (*state statutes*) und auf lokaler Ebene von Städten, Kreisen oder Gemeinden (*local ordinances*).[993] Im Falle eines Konflikts gilt auch in den USA „Bundesrecht bricht Landesrecht".[994]

aa) Gesetzgebung

In den USA können auf Bundesebene beide Kammern des Kongresses, also das Repräsentantenhaus sowie der Senat, Gesetzesentwürfe (*bills*) einbringen.[995]

Der jeweilige Gesetzesentwurf wird nach Annahme durch die initiierende Kammer an die jeweils andere Kammer weitergeleitet und dort von einem Komitee (*Committee*), in dessen Zuständigkeit der Gesetzesentwurf fällt, untersucht.[996] Stimmt die jeweils andere Kammer dem Gesetzesentwurf zu, so muss dieser von beiden Kammern in identischer Form verabschiedet werden und wird erst daraufhin an den Präsidenten weitergeleitet, durch dessen Unterschrift der Entwurf zum Gesetz wird.[997] Hat eine Kammer hingegen nach entsprechender Untersuchung Änderungswünsche, wird zunächst eine Art Vermittlungsausschuss (*Conference Committee*) errichtet.[998]

Sowohl der Senat als auch das Repräsentantenhaus verfügen über diverse spezialisierte Ausschüsse (*committees*), welche u.a. damit betraut sind für den jeweils zuständigen Aufgabenbereich Anhörungen durchzuführen, Gesetzesentwürfe zu erarbeiten und zu untersuchen.[999] In diesem Zusammenhang fertigen sie auch Reports zu Gesetzesentwürfen an, welche die Hintergründen des

---

[992] Code of Laws of the United States of America, abgekürzt U.S.C.
[993] Hay, Law of the U.S., Rn. 18.
[994] Reiley/de la Vega, S. 39.
[995] Eine detaillierte Darstellung zur Gesetzgebung findet sich in dem Dokument H. Con. Res. 190 des 110ten Kongresses „How our laws are made", einsehbar unter http://www.gpo.gov/fdsys/pkg/CDOC-110hdoc49/pdf/CDOC-110hdoc49.pdf, zuletzt besucht am 24.04.2016.
[996] Hay, Law of the U.S., S. 21.
[997] Hay. Law of the U.S., S. 21.
[998] Hay. Law of the U.S., S. 21.
[999] Siehe hierzu https://www.congress.gov/help/legislative-glossary/#glossary_committeesubcommittee, zuletzt besucht am 24.04.2016.

Gesetzesentwurfs erläutern und weitere Orientierung hinsichtlich dem Sinn und Zweck des Gesetzesentwurfs mit seinen einzelnen Vorschriften bieten.[1000]

bb) Gesetzesauslegung

Im Gegensatz zu anderen *common law* Ländern, wie bspw. Australien, gibt es in den USA keine offiziellen Auslegungsmaximen, sondern lediglich eine Mixtur unterschiedlicher durch die Gerichte entwickelter Herangehensweisen.[1001]

Es kommen grundsätzlich die folgenden Herangehensweisen in Betracht: Wortlaut (*plain meaning)*, Entstehungsgeschichte (*legislative history*), sozialer Zweck (*social purpose*) und Kontext (*Context of Statutory Laguage*).[1002]

Als Faustformel lässt sich sagen, dass Gerichte sich grundsätzlich am Wortlaut einer Vorschrift in einer Art und Weise orientieren, die gleichzeitig dem Zweck der Vorschrift Rechnung trägt.[1003]

Insbesondere im Bereich des Urheberrechts wird dabei oft auf die Gesetzgebungshistorie, also die *House* und *Senate Reports* zu dem jeweiligen Gesetzesentwurf, zurückgegriffen.[1004]

2. Gerichtsbarkeit

Die USA verfügt über ein zweigliedriges Gerichtssystem, mit Gerichten auf Bundesebene (*federal courts*) und in den einzelnen Bundesstaaten (*state courts*).[1005]

Die Kompetenzen der *federal courts* ergeben sich aus Art. 3 Abs. 2 der Verfassung. Demnach sind sie vor allem für sog. *federal question cases* und *diversity cases* zuständig.[1006] Ersteres sind

---

[1000] Je nachdem ob der Report von einem Committee des Senates oder Repräsentantenhauses stammt, ist entweder die Rede von dem *Senate Report* oder dem *House Report*. Eine übersichtliche visuelle Veranschaulichung des Gesetzgebungsverfahrens in den USA befindet sich auf der Homepage des Kongresses unter https://www.congress.gov/legislative-process, zuletzt besucht am 24.04.2016.

[1001] Burnham, Introduction to U.S. Law, S. 54.

[1002] Burnham, Introduction to U.S. Law, S. 54 ff.

[1003] Burnham, Introduction to U.S. Law, S. 54.

[1004] Finlay-Hunt, Colum. Bus. L. Rev. 906, 935 (2013).

[1005] Burnham, Introduction to U.S. Law, S. 167.

[1006] Reiley/de la Vega, S. 10.

Streitigkeiten, die sich aus der Verfassung oder sonstigem Bundesrecht ergeben, letzteres Streitigkeiten zwischen Bürgern verschiedener Bundesstaaten, sofern der Streitwert $ 75.000 übersteigt.[1007]

Die ausschließliche Zuständigkeit der Bundesgerichte für das Urheberrecht ist in Title 28 U.S.C. *Judiciary and Judicial Procedure* geregelt.[1008]

3. U.S.-amerikanisches Urheberrecht

Auch das U.S.-amerikanische Urheberrecht hat seine Wurzeln im englischen Recht.[1009]

Der Kongress hat gem. Art. 1 Abs. 8 der Verfassung Gesetzgebungskompetenz in Urheberrechtssachen.[1010]

Das erste im Jahr 1790 auf Bundesebene erlassene U.S.-amerikanische Urheberrechtsgesetz basiert auf der *Statute of Anne* (*1710*)[1011] Großbritanniens und wurde in dem Jahrhundert nach Inkrafttreten insbesondere im Hinblick auf den Schutzgegenstand sukzessive erweitert und schließlich durch den *Copyright Act of 1909* ersetzt.[1012]

Dessen Nachfolger, der *Copyright Act of 1976,* stellt das derzeit geltende Urheberrechtsgesetz dar und befindet sich in Title 17 U.S.C.

II. Allgemeine Haftungsregeln

1. Direct und indirect infringer

Das U.S.-amerikanische Urheberrecht unterscheidet grundsätzlich zwischen dem *direct infringer* und dem *secondary infringer*. Während die unmittelbare Haftung für Urheberrechtsverletzungen in 17 U.S.C. § 501 (a) geregelt ist, wurde die mittelbare Haftung

---

[1007] Reiley/de la Vega, S. 10.
[1008] 28 U.S.C. § 1498 (b).
[1009] Gorman, Copyright Law, S. 1.
[1010] *„The Congress shall have power [...] to promote the progress of science and useful arts, by securing for limited times to authors and inventors the exclusive right to their respective writings and discoveries [...].“*
[1011] *„An act for the encouragement of learning, by vesting the copies of printed books in the authors or purchasers of such copies, during the times therein mentioned.“*
[1012] Gorman, Copyright Law, S. 2.

durch *case law* entwickelt. Im Rahmen der mittelbaren Haftung entstanden zwei Haftungstheorien: *contributory liability* und *vicarious liability*. Erst später hinzu gekommen ist die *vicarious liability*.

a) Direct Infringer

Gem. 17 U.S.C. § 501 (a) ist derjenige, der ein exklusives Recht des Urheberrechtsinhabers verletzt, als Verletzer (*infringer*) anzusehen.

Fälle von *direct infringement* im Urheberrecht sind grundsätzlich verschuldensunabhängig.[1013] Man spricht insofern von einer *strict liability*.[1014] Dennoch hat 1995 erstmals der *N.D. California* im Hinblick auf die unmittelbare Verantwortlichkeit eines Access-Providers ein weiteres Merkmal hinzugefügt und zwar *some element of volition or causation.*[1015] Ohne dieses Element des Willens oder der Kausalität würde der Kreis der potentiellen *direct infringer* ins Uferlose gehen.[1016] Es mache keinen Sinn, in Fällen, in denen ein Dritter eine Urheberrechtsverletzung begangen habe, einen Maßstab anzuwenden, der dazu führt, dass unzählige andere Parteien für die gleiche Rechtsverletzung als *direct infringer* angesehen werden.[1017] Andere Gerichte sind diesem Grundsatz gefolgt.[1018] So hat beispielsweise der *Fourth Circuit* bestätigt, dass eine entsprechende Interpretation des *Copyright Acts* geboten sei, da zwar keine vorsätzliche Verletzung vorausgesetzt werde, wohl aber *„conduct by a person"*.[1019] Das automatische Kopieren, Speichern und die automatische Durchleitung von urheberrechtlich

[1013] Religious Technology Center v. Netcom On-Line Communication Services, Inc., 907 F.Supp. 1361, 1367 (1995); Scott on Multimedia Law, § 4.37 [A] Direct Infringement, „*It does not matter that [the defendant, Anmerkung des Verfassers] may have been unaware of the copyright infringement. Intent to infringe is not needed to find copyright infringement*."

[1014] Scott on Multimedia Law, § 4.37 [A] Direct Infringement.

[1015] Religious Technology Center v. Netcom On-Line Communication Services, Inc., 907 F.Supp. 1361, 1370 (1995).

[1016] Religious Technology Center v. Netcom On-Line Communication Services, Inc., 907 F.Supp. 1361, 1372 (1995).

[1017] Religious Technology Center v. Netcom On-Line Communication Services, Inc., 907 F.Supp. 1361, 1372 (1995).

[1018] Cartoon Network LP, LLLP v. CSC Holdings, Inc., 536 F.3d 121 (2008); Costar Group, Inc. v. Loopnet, Inc., 373 F.3d 544 (4th Cir. 2004).

[1019] Costar Group, Inc. v. Loopnet, Inc., 373 F.3d 544, 549 (4th Cir. 2004).

geschütztem Material stelle hingegen keine solche willentliche Handlung (*volitional conduct*) dar.[1020]

Auch das Repräsentantenhaus schließt sich in einem früheren Report zum DMCA der Argumentation des Gerichts im „Netcom"-Fall an und weist damit etwaig gegenläufige Auffassungen inzidenter zurück.[1021]

Kenntnis der Rechtsverletzung ist für die unmittelbare Haftung nicht erforderlich.[1022]

b) Indirect Infringer

Neben dem *direct infringer* kann der Urheber auch gegen *indirect infringer* vorgehen im Rahmen der sog. *secondary liability* (subsidiäre/mittelbare Haftung).

Die Haftungsfigur der *secondary liability* ist nicht im amerikanischen Urheberrechtsgesetz festgeschrieben.[1023] Sie entstammt ursprünglich dem Bereich des Deliktsrechts und wurde so im Rahmen des Urheberrechts, als Teil des Deliktsrechts, von den Gerichten weiterentwickelt.[1024]

Teilweise wird auch aus dem Text des amerikanischen Urheberrechtsgesetzes ein Hinweis auf die mittelbare Haftung abgelesen und zwar in der Verwendung des Wortes *to authorize* in § 106, welches in den Copyright Act von 1976 inkorporiert wurde.[1025]

aa) Contributory Infringement

Im Bereich des Urheberrechts hat der *Supreme Court* das Prinzip der *contributory liability* im Jahr 1984 erstmals offiziell anerkannt.[1026] Voraussetzung hierfür ist, dass der *contributory infringer* (1) Kenntnis von der direkten Rechtsverletzung hat

[1020] Costar Group, Inc. v. Loopnet, Inc., 373 F.3d 544, 551 (4th Cir. 2004).
[1021] H.R. Rep. 105-551(I), S. 26.
[1022] Scott on Multimedia Law, § 4.37 [A] Direct Infringement.
[1023] Gorman, Copyright Law, S. 131; anders im Patentrecht, hier ist die *secondary liability* in 35 U.S.C. § 271 (b) und (c) geregelt.
[1024] Helman, 19 Tex. Intell. Prop. L.J. 111, 114 f. (2010).
[1025] Leaffer, § 9.07 [A]; Cohen/Loren/Okediji/O'Rourke, S. 479; Nimmer on Copyright, § 12.04 [A]; *„Subject to sections 107 through 122, the owner of copyright under this title has the exclusive rights to do and to authorize any of the following: [...]."*
[1026] Sony Corp. v. Universal City Studios, 104 S.Ct. 774 (1984).

(*knowledge*) und (2) er diese eingeleitet, verursacht oder maßgeblich zu dieser beigetragen hat (*material contribution*).[1027]

Kenntnis im Sinne der contributory liability bedeutet entweder tatsächliche Kenntnis (*actual knowledge*) oder Kennenmüssen (*constructive knowledge*).[1028]

Umfasst sind hiervon demnach auch Fälle von *willful blindness*, d.h. das bewusste Augen verschließen.

Grundsätzlich sind zwei verschiedene Aktivitäten, welche als *material contribution* Anlass zu einer Verantwortlichkeit als *contributory infringement* geben, zu unterscheiden: (1) Persönliches Verhalten, welches die Rechtsverletzung fördert oder diese unterstützt und (2) die Zurverfügungstellung von Produkten, welche die Rechtsverletzung ermöglichen.[1029]

Die Hürde für eine *material contribution* ist grds. recht niedrig anzusetzen, hierfür genügt es bspw. wenn von dem ISP *site and facilities* für die Rechtsverletzungen eines Dritten bereitgestellt werden.[1030]

Als Ausnahme von der Zurverfügungstellung von Produkten, welche eine Rechtsverletzung ermöglichen, gilt die sog. *Sony-Doktrin*.

In *Sony v. Universal*[1031] hat der *Supreme Court* sich mit der Frage der *contributory infringement* im Rahmen des Verkaufs von VHS-Rekordern befasst. Nachdem er zunächst grundsätzlich die Haftung des mittelbaren Verletzers im Urheberrecht bestätigte, griff er in

---

[1027] Gershwin Pub. Corp. v. Columbia Artists Management, Inc., 443 F.2d 1159, 1162 (1971), *„[...] one who, with knowledge of the infringing activity, induces, causes or materially contributes to the infringing conduct of another, may be held liable as a ‚contributory' infringer."*

[1028] Ellison v. Robertson, 357 F.3d 1072, 1076 (9th Cir. 2004); Ballon, Internet & E-Commerce, 4.11[3] [A].

[1029] Nimmer on Copyright, § 12.04 [A] [3].

[1030] Capitol Records, Inc. v. MP3Tunes, LLC, 821 F.Supp.2d 627, 648 (S.D.N.Y. 2011); für den Offline-Bereich: Fonovisa, Inc. v. Cherry Auction, Inc., 76 F.3d 259, 264 (9th Cir. 1996); *Material contribution* wurde lediglich abgelehnt für die Mitwirkung eines Bezahldienstes, da die rechtsverletzenden Inhalte weder über dessen Dienst vermittelt wurden noch dafür genutzt werden konnten, rechtsverletzendes Material zu lokalisieren („*[...] services provided by the credit card companies do not help locate and are not used to distribute the infringing images. [...] Even if infringing images were not paid for, there would still be infringement.*"), siehe Perfect 10, Inc. v. Visa Intern. Service Ass'n, 494 F.3d 788, 796 (9th Cir. 2007).

[1031] Sony Corp. v. Universal City Studios, 104 S.Ct. 774 (1984).

der Folge auf ein Institut des Patentrechts zurück, die sog. *staple article of commerce doctrine*[1032]. Danach ist der Hersteller eines Produktes kein *contributory infringer*, sofern das Produkt wesentlich für nicht rechtsverletzende Nutzungen geeignet ist (*staple article or commodity of commerce suitable for substantial noninfringing use*). Das Gericht führt hier aus, dass obwohl es signifikante Unterschiede zwischen dem Urheber- und dem Patentrecht gibt, die *staple article of commerce doctrine* für das richtige Gleichgewicht zwischen den legitimen Interessen der Urheberrechtsinhaber und der Hersteller sorgt.[1033]

Daher stelle es keinen Fall der *contributory infringement* dar, wenn das Produkt weitgehend für legitime und unbedenkliche Zwecke verwendet werden könne.[1034]

Es ist strittig, ob die *Sony-Doktrin* nicht nur auf das Vorhalten von Produkten sondern auch von Services Anwendung findet, so dass auch ISP in den Anwendungsbereich fallen.[1035]

bb) Vicarious Infringement

Eine mittelbare Haftung kann zudem im Sinne der *vicarious infringement* vorliegen. Demnach kann ein Dritter für eine Rechtsverletzung mittelbar verantwortlich sein, sofern er (1) das Recht und die Möglichkeit hat, die rechtsverletzende Aktivität zu überwachen bzw. zu kontrollieren und (2) ein direktes finanzielles Interesse an einer solchen rechtsverletzenden Aktivität hat.[1036] Eine Kenntnis der Rechtsverletzung ist, anders als bei der *contributory liability*, nicht erforderlich.[1037]

[1032] 35 U.S.C. § 271 (c).
[1033] Sony Corp. v. Universal City Studios, 104 S.Ct. 774, 788f. (1984).
[1034] Sony Corp. v. Universal City Studios, 104 S.Ct. 774, 789 (1984); Teilweise wird auch eine Anwendbarkeit der Sony-Doktrin für Fälle von *vicarious liability* befürwortet, so bspw. Liu, Vanderbilt Journal of Entertainment and Technology Law, 343, 555 (2005) sowie Miles, 19 Berkeley Tech. L.J. 21, 50 (2004).
[1035] Dafür: Perfect 10 v. Google, Inc., 416 F.Supp. 2d 828, 853 (C.D. Cal. 2006); Liu, Vanderbilt Journal of Entertainment and Technology Law, 343, 555 (2005); Eher dagegen aufgrund der „ongoing relationship" zwischen ISP und Nutzer: Arista Records LLC v. Usenet.com, Inc, 633 F.Supp. 2d 124, 153 (S.D.N.Y. 2009); Capitol Records, Inc. v. MP3Tunes, LLC, 821 F.Supp.2d 627, 649 (S.D.N.Y. 2011).
[1036] Shapiro, Bernstein & Co. v. H. L. Green Co., 316 F.2d 304, 307 (1963).
[1037] Reese, 34 Sw. U. L. Rev. 287, 304 (2004).

In *Napster* hat der *Ninth Circuit* eine Kontrollmöglichkeit angenommen aufgrund der Möglichkeit, den Zugang der Rechtsverletzer zu dem Service von Napster zu blockieren und deren Benutzerkonto zu löschen.[1038] Auch ein finanzieller Vorteil sei aufgrund der Tatsache anzunehmen, dass Napsters zukünftiger Umsatz abhängig sei von der Anzahl der Nutzer und den von diesen hochgeladenen Musikdateien.[1039]

cc) Inducement Liability

Im Jahr 2005 hat sich der *Supreme Court* erneut mit der Frage der *secondary liability* im Urheberrecht befasst und als Folge die sog. *inducement liability*[1040] eingeführt.[1041] Danach ist derjenige, *„who distributes a device with the object of promoting its use to infringe copyright, as shown by clear expression or other affirmative steps taken to foster infringement, [...] liable for the resulting acts of infringement by third parties.“*[1042]

Die *inducement liability* ist durch vier Merkmale gekennzeichnet:[1043]

(1) *Distribution of a device or product* (Vertrieb eines Gegenstandes oder Produktes),

(2) *acts of infringement* (Verletzungshandlung),

(3) *object of promoting its use to infringe* copyright (Absicht durch den Gegenstand/das Produkt urheberrechtswidrige Nutzungen zu fördern),

(4) *causation* (Kausalität).

In *Fung v. Columbia* bestätigte der *Ninth Circuit* die Anwendbarkeit der *inducement liability* auf ISP, welche Services anbieten.[1044]

[1038] A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1023 (9th Cir. 2001).
[1039] A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1023 (9th Cir. 2001).
[1040] Englischer Begriff „inducement“ = Veranlassung, Ansporn.
[1041] Metro-Goldwyn-Mayer Studios Inc. v. Grokster, 125 S.Ct. 2764 (2005).
[1042] Metro-Goldwyn-Mayer Studios Inc. v. Grokster, 125 S.Ct. 2764, 2780 (2005).
[1043] Metro-Goldwyn-Mayer Studios Inc. v. Grokster, 125 S.Ct. 2764, 2764 (2005).
[1044] Columbia Pictures Industries, Inc. v. Fung, 710 F.3d 1020, 1021 (9th Cir.

Umstritten ist die genaue Einordnung der *inducement liability*. Teilweise wird sie als Unterfall der *contributory liability* behandelt, teilweise als eigenständige Form der mittelbaren Haftung neben der *contributory* und *vicarious liability*.[1045]

Die Befürworter einer Einordnung unter die *contributory liability* stützen sich hauptsächlich auf die klassische Definition dieser, in welcher ausdrücklich *inducement* erwähnt wird.[1046] Sofern jedoch *inducement* im Rahmen des *contributory infringement* eine Rolle spielt, so ist es hier von Nöten, dass dem Beklagten nachgewiesen wird, dass sein Verhalten tatsächlich die streitgegenständliche Rechtsverletzung herbeigeführt hat.[1047] Im Gegensatz hierzu genügt es für die *inducement liability* nach *Grokster*, wenn der Beklagte eine entsprechend subjektive Absicht zur Veranlassung einer Urheberrechtsverletzung verfügte.[1048] Es ist nicht notwendig, dass diese Absicht in direkter Verbindung mit der jeweiligen Rechtsverletzung steht.[1049]

Die Ansicht, dass *inducement* eine von der *contributory infringement* unabhängige Form der *secondary liability* darstellt, wird auch durch die Ausführungen des *Supreme Courts* in *Grokster* gestützt. So führt dieser bereits zu Beginn aus, dass das „Sony"-Urteil nicht andere mittelbare Haftungstheorien verdrängt habe.[1050] Vielmehr hat der *Supreme Court* die *inducement rule* aus dem Patentrecht übernommen, wo diese eine neben dem *contributory infringement* unabhängige Form der mittelbaren Haftung

---

2013).

[1045] Für eine Einordnung unter die *contributory liability*: Perfect 10, Inc. v. Amazon.com, Inc., 508 F.3d 1146, 1171 (2007); Flava Works, Inc. v. Gunter, 689 F.3d 754, 759 (2012); wohl auch Scott on Information Technology, § 2.51 [C] Infringement; für eine Einordnung als eigenständige Form der *secondary liability*: Nimmer on Copyright, § 12.04 [A] [4] [b]; Blevins, 34 Cardozo L. Rev. 1821, 1848 (2013); Yen, 91 Minn. L. Rev. 184, 227 (2006); Ballon, E-Commerce & Internet Law (2014-2015 Update), 4.11[3][A].

[1046] *„One who, with knowledge of the infringing activity, induces, causes or materially contributes to the infringing conduct of another, may be held liable as a ‚contributory' infringer."*

[1047] Nimmer on Copyright, § 12.04 [A] [4] [b].

[1048] Nimmer on Copyright, § 12.04 [A] [4] [b].

[1049] Nimmer on Copyright, § 12.04 [A] [4] [b].

[1050] Metro-Goldwyn-Mayer Studios Inc. v. Grokster, 125 S.Ct. 2764, 2768 (2005).

darstelle.[1051] Nichts anderes gilt entsprechend auch für den Bereich des Urheberrechts.

c) Rechtsfolgen

Die Rechtsbehelfe bei einer erfolgten Urheberrechtsverletzung sind in 17 U.S.C. §§ 502 bis 506 geregelt. Es wird hinsichtlich der Rechtsbehelfe nicht unterschieden, ob es sich um einen *direct* oder *indirect infringer* handelt.

aa) Unterlassung - Injunctions

Nach 17 U.S.C. § 502 kann ein Gericht eine vorläufige oder finale Anordnung erlassen, die es für angemessen hält, um eine Urheberrechtsverletzung zu verhindern oder zu beschränken. Solche Anordnungen kann das Gericht nach Ermessen anordnen, eine erfolgte Urheberrechtsverletzung berechtigt nicht automatisch zu einer (Unterlassungs-) Anordnung.[1052] Eine Anordnung muss vielmehr einem 4 Faktoren-Test genügen, nach dem der Antragsteller folgendes darzulegen hat: (1) dass er einen irreparablen Schaden erlitten hat, (2) dass die nach dem Gesetz zustehenden Rechtsbehelfe, wie bspw. Schadensersatz, unzureichend sind, um diesen Schaden zu kompensieren, (3) dass, unter Berücksichtigung der beiderseitigen Belastungen durch eine Anordnung, eine solche gerechtfertigt ist und (4) dass die öffentlichen Interessen nicht beeinträchtigt werden.[1053]

bb) Schadensersatz – Damages

Nach 17 U.S.C. § 504 haftet der Verletzer zudem auf Schadensersatz. Der Verletzte hat die Wahl zwischen dem tatsächlichen Schaden und Gewinn (*actual damages and profits*)[1054] sowie eines gesetzlich festgelegten Schadensersatzes (*statutory damages*)[1055].

[1051] Metro-Goldwyn-Mayer Studios Inc. v. Grokster, 125 S.Ct. 2764, 2780 (2005).
[1052] New York Times Co. v. Tasini, 533 U. S. 483, 505 (2001).
[1053] Ebay Inc. v. MercExchange, L.L.C. 547 U.S. 388 (2006).
[1054] 17 U.S.C. § 504 (b).
[1055] 17 U.S.C. § 504 (c).

Ersteres bedeutet, dass der Urheberrechtsinhaber sowohl den tatsächlich erlittenen Schaden als auch zusätzlich den Gewinn des Rechtsverletzers ersetzt verlangen kann.[1056] Entscheidet er sich für den gesetzlich festgelegten Schadensersatz, so kann er diese Entscheidung jederzeit vor Erlass des Urteils dem Gericht anzeigen. Die Höhe des gesetzlich festgesetzten Schadensersatzanspruches beträgt nicht weniger als $ 750 und nicht mehr als $ 30.000 pro verletztem Werk.[1057] Es ist unerheblich ob und in welcher Höhe dem Urheberrechtsinhaber tatsächlich ein Schaden entstanden ist. Die Festsetzung der Höhe liegt im Ermessen des Gerichts. In Fällen in denen der Rechtsverletzer die Rechtsverletzung vorsätzlich (*willfully*) begangen hat, kann das Gericht einen Schadensersatz von bis zu $ 150.000 pro Werk zusprechen.[1058] Im Falle eines ahnungslosen Rechtsverletzers (*innocent infringer*) kann der Schadensersatzanspruch auf nicht weniger als $ 200 pro Werk reduziert werden.[1059] Dem Verletzer obliegt hier die Pflicht nachzuweisen, dass er nichts von der Rechtsverletzung wusste und er keinen Grund hatte zu glauben, dass sein Handeln eine Urheberrechtsverletzung begründen könnte.[1060]

III. Haftungsprivilegien nach § 512 DMCA

Die Haftungsprivilegien der ISP für Urheberrechtsverletzungen ihrer Nutzer sind im U.S.-amerikanischen Recht unmittelbar im U.S.-amerikanischen Urheberrechtsgesetz in 17 U.S.C. § 512 verankert und gelten somit nur für den Bereich des Urheberrechts.
§ 512 DMCA entfaltet damit seine Wirkung nur bezüglich Urheberrechtsverletzungen. Vereinzelt gibt es jedoch weitere Haftungsprivilegien für ISP bezüglich anderweitiger Rechtsverletzungen.[1061]

[1056] Nimmer on Copyright, § 14.01 [A].
[1057] 17 U.S.C. § 504 (c) (1).
[1058] 17 U.S.C. § 504 (c) (2).
[1059] 17 U.S.C. § 504 (c) (2).
[1060] 17 U.S.C. § 504 (c) (2).
[1061] Bspw. 47 U.S.C. § 230 („Communications Decency Act“) bzgl. Persönlichkeitsrechtsverletzungen, 15 U.S.C. § 1114 (2) („Lanham Act“) bzgl.

Die Privilegien finden Anwendung, wenn ein ISP nach geltendem Recht haftet und schränken die möglichen Rechtsfolgen ein.[1062]

1. Gesetzgebungsgeschichte

Die rasante Entwicklung neuer Technologien und die weltweite Verbreitung des Internets bewegte die US-amerikanische Regierung unter Präsident Clinton dazu, im Februar 1993 eine *Information Infrastructure Task Force* (IITF) zu bilden.[1063] Die IITF bestand aus drei unterschiedlichen Ausschüssen: dem *Telecommunications Policy Committee*, dem *Committee on Applications and Technology* und dem *Information Policy Committee* mit jeweils eigenständigen, klar abgegrenzten Aufgabenbereichen.[1064] Innerhalb des Letzteren wurde die Arbeitsgruppe *Working Group on Intellectual Property Rights* gebildet, um die Auswirkungen auf das geistige Eigentum, insbesondere das Urheberrecht, zu untersuchen und Änderungen des bestehenden U.S.-Rechts zur Anpassung an die Bedürfnisse der Informationsgesellschaft vorzuschlagen.[1065]

Die Arbeitsgruppe veröffentlichte 1995 einen Report (*White Paper*) mit konkreten gesetzlichen Vorschlägen, um das Urheberrecht für die neu aufkommenden Technologien zu rüsten. Auch gesetzliche Haftungsprivilegien für ISP wurden in dem *White Paper* diskutiert, letzten Endes jedoch ausdrücklich abgelehnt.[1066]

Als Begründung wurde angeführt, dass ISP zwar eine wesentliche Rolle in der Entwicklung der Informationsinfrastruktur spielen, dass dies aber kein Grund dafür sei, sie von ihrer Verantwortlichkeit zu befreien, da sie ihre Funktion auch ausführen könnten, ohne dabei die Urheberrechte anderer zu verletzen oder solche Urheberrechtsverletzungen zu fördern.[1067] Da ISP in einer

---

Markenrechtsverletzungen.

[1062] H.R. Rep. 105-551(II), S. 50.

[1063] Ziel dieser Task Force war es *„to articulate and implement the Administration's vision for the National Information Infrastrucutre (NII)"*, siehe Information Infrastructure Task Force, S. 1.

[1064] Information Infrastructure Task Force, S. 1.

[1065] Information Infrastructure Task Force, S. 2.

[1066] Information Infrastructure Task Force, S. 122.

[1067] Information Infrastructure Task Force, S. 117.

geschäftlichen Verbindung zu Ihren Nutzern stehen, seien sie in der besseren Lage, Urheberrechtsverletzungen vorzubeugen oder abzustellen.[1068]

Im September 1995 präsentierten sowohl der Senat als auch das Repräsentantenhaus einen Gesetzesentwurf, welcher die Änderungsvorschläge des *White Papers* aufgriff.[1069] Die Gesetzesentwürfe durchliefen mehrere Anhörungen und wurden begleitet von Verhandlungen zwischen den unterschiedlichen Interessenvertretern, kamen allerdings zum Stillstand, da sich Vertreter von Urhebern und ISP nicht hinsichtlich der Problematik der Haftung der ISP für Rechtsverletzungen ihrer Nutzer einigen konnten.[1070]

In der Zwischenzeit schritten internationale Bemühungen zur Sicherung von Urheberrechten im digitalen Zeitalter voran. In der Folge wurden im Dezember 1996 zwei essentielle multilaterale Abkommen geschlossen: das WIPO-Urheberrechtsabkommen (WCT) und der WIPO-Vertrag über Darbietungen und Tonträger (WPPT). Aber diese Abkommen enthielten keine expliziten Regelungen hinsichtlich der Verantwortlichkeit von ISP für Urheberrechtsverletzungen ihrer Nutzer.

Im Zuge der Umsetzung der WIPO-Abkommen in nationales Recht entschied sich der Kongress abermals das Thema der Haftungsbegrenzung für ISP anzugehen und führte 1997 zwei Gesetzesentwürfe[1071] ein, welche die Grundlage für den *Digital Millenium Copyright Act*[1072] (DMCA) bildeten. Title II des DMCA, der „Online Copyright Infringement Liability Limitation Act" (OCILLA), enthielt die heutigen Haftungsprivilegien für ISP, welche in 17 U.S.C. § 512 „Limitations on liability relating to

[1068] Information Infrastructure Task Force, S. 117.
[1069] S. Rep. 105-190, S. 2.
[1070] S. Rep. 105-190, S. 4.
[1071] H.R. 2180, S. 1146. Wie unter D.I.1.b)aa) erläutert, haben beide Kammern des Kongresses, das Repräsentantenhaus und der Senat, eine Gesetzgebungsinitiative. Jeder Gesetzgebungsvorschlag muss am Ende jedoch identisch von beiden Kammern verabschiedet werden, um dem Präsidenten übermittelt zu werden und durch dessen Unterschrift, im Falle einer Annahme, Rechtskraft zu entfalten.
[1072] Pub. L. No. 105-304, 112 Stat. 2860 (Oct. 28, 1998).

material online“[1073] umgesetzt wurden. Diese werden umgangssprachlich als *safe harbor* (sicherer Hafen) bezeichnet. Erklärtes Ziel ist die Stärkung der Zusammenarbeit von Urheberrechteinhabern und ISP bei Auffindung und Umgang mit Online-Urheberrechtsverletzungen.[1074] Zugleich soll den ISP mehr Rechtssicherheit zukommen hinsichtlich einer potentiellen Verantwortlichkeit für solche Urheberrechtsverletzungen.[1075]

2. Anwendungsbereich

§ 512 DMCA regelt die Haftungsprivilegierung der ISP bei Urheberrechtsverletzungen durch Dritte.

Die Privilegien greifen in Fällen, in denen der ISP nach den allgemeinen Grundsätzen verantwortlich gemacht werden kann. Umfasst hiervon sind lt. der Gesetzesgebungsmaterialien sowohl eine Haftung wegen *direct*, *vicarious* oder *contributory infringement*.[1076] Es ist fraglich, ob auch die erst später konstruierte *inducement liability* von den *safe harbor*-Privilegien erfasst ist.[1077] Die Befürworter einer Anwendbarkeit der safe harbor-Privilegien auf Fälle von *inducement liability* orientieren sich hauptsächlich an den Gesetzgebungsmaterialien, welche alle bis dato bestehenden Haftungskonstrukte dem Anwendungsbereich des DMCA unterwerfen.[1078] Die Vertreter der Gegenansicht akzentuieren die inhärente Gegensätzlichkeit der Privilegien und der *inducement liability*.[1079] Während die *safe harbor*-Privilegien geschaffen wurden, um das passive Betreiben eines legitimen Internetgeschäftes in gutem Glauben zu betreiben, basiere die

[1073] Nachfolgend § 512 DMCA genannt.
[1074] H.R. Rep. 105-551(II), S. 49; S. Rep. 105-190, S. 20.
[1075] H.R. Rep. 105-551(II), S. 49 f.; S. Rep. 105-190, S. 20.
[1076] H.R. Rep. 105-551(II), S. 50; S. Rep. 105-190, S. 20.
[1077] Dafür: Ninth Circuit in Columbia Pictures Indistries, Inc. v. Fung, 710 F.3d. 1020, 1039 (9th Cir. 2013); Blevins, 34 Cardozo L. Rev. 1821, 1881 (2013); Dagegen: Finley-Hunt, 2013 Colum. Bus. L. Rev. 906, 908; Mazoki, 30 Tem. J. Sci. Tech. & Envtl. 275, 307 (2011).
[1078] Columbia Pictures Indistries, Inc. v. Fung, 710 F.3d. 1020, 1039 (9th Cir. 2013).
[1079] Mazoki, 30 Tem. J. Sci. Tech. & Envtl. 275, 307 (2011).

inducement liability gerade auf dem aktiven arglistigen Verhalten des Providers zur Förderung von Rechtsverletzungen.[1080]

Im Hinblick auf die Gesetzgebungsgeschichte ist jedoch davon auszugehen, dass die *safe habor*-Privilegien jegliche Art potentieller Haftung umfassen sollten. Auch wenn davon auszugehen ist, dass im Rahmen der Prüfung der verschiedenen Voraussetzungen des DMCA, solche ISP, die Rechtsverletzungen aktiv fördern, regelmäßig aus dem Anwendungsbereich herausfallen, sind dennoch Konstellationen möglich, in denen dem ISP berechtigterweise der Schutz des DMCA zugesprochen werden kann.[1081]

Fällt ein ISP unter die Privilegien des § 512 DMCA, befreit ihn dies von jeglichen Schadensersatzansprüchen. Zudem sind die potentiellen Anordnungen beschränkt auf die unter § 512 (j) DMCA geregelten Fälle.[1082]

3. Adressaten

Adressaten der Haftungsprivilegien des § 512 DMCA sind nicht lediglich die ISP als Unternehmen, sondern auch deren Mitarbeiter, sofern diese im Rahmen ihrer Beschäftigung handeln.[1083]

4. Dogmatische Einordnung

Der Großteil der U.S.-amerikanischen Gerichte scheint davon auszugehen, dass in einem ersten Schritt die Haftung des jeweiligen ISP nach den allgemeinen Grundsätzen zu prüfen ist und in einem zweiten Schritt die Haftungsprivilegien, welche die

---

[1080] Mazoki, 30 Tem. J. Sci. Tech. & Envtl. 275, 307 (2011).

[1081] Columbia Pictures Indistries, Inc. v. Fung, 710 F.3d. 1020, 1040 (9th Cir. 2013).

[1082] Siehe hierzu S. 349.

[1083] Hendrickson v. Ebay, Inc., 165 F. Supp. 2d 1082, 1093 f. (D.C. Cal. 2001), *„The copyright claims against eBay's employees [...] are based solely on alleged acts and omissions in the course and scope of their employment with eBay. Consequently, eBay's immunity from liability for copyright infringement should also extend to [these employees, Anmerkung des Verfassers]. To hold that the safe harbor provisions of the DMCA protects the company but not its employees for the same alleged bad acts would produce an absurd result. Congress could not have intended to shift the taret of infringement actions from the Internet service providers to their employees when it enacted the safe harbor provisions."*

Rechtsfolgen stark einschränken.[1084] Auch die Gesetzgebungsmaterialien lassen auf eine entsprechende Interpretation als sog. Nachfilter schließen.[1085]

In der Literatur findet die dogmatische Einordnung der Haftungsprivilegien wenig Beachtung. Lediglich vereinzelt wird für eine vorgelagerte Prüfung der Haftungsprivilegien plädiert, mit der Begründung, dass im Ergebnis eine Haftung der ISP eher bejaht werden würde, wenn zunächst die allgemeinen Haftungsgrundsätze geprüft werden.[1086] *Bretan* führt als Beispiele für diese These *A&M Records v. Napster*[1087], *Ellison v. Robertson*[1088] und *Perfect 10 v. Cybernet Ventures*[1089] an.[1090] Ob die zitierten Fälle tatsächlich als Nachweis dafür dienen können, dass Gerichte eher geneigt sind, eine Haftung der ISP zu bejahen, wenn sie deren Rolle zuvor durch die Linse der allgemeinen Haftungsgrundsätze betrachtet haben, ist aber fraglich. *Bretan* versäumt es, nachvollziehbare Belege für ihre These zu liefern. So wurde bspw. *Cybernet* der DMCA *safe harbor* verwehrt, da das Gericht der Auffassung war, *Cybernet* habe seine *repeat infringer policy* nicht angemessen umgesetzt, was allerdings Voraussetzung für die Inanspruchnahme der Privilegien ist.[1091]

[1084] So z.B. Perfect 10, Inc. v. Cybernet Ventures, Inc., 213 F.Supp.2d 1146 (2002); Ellison v. Robertson, 357 F.3d 1072 (9th Cir. 2004), Columbia Pictures Indistries, Inc. v. Fung, 710 F.3d. 1020 (9th Cir. 2013); grundsätzlich zustimmend, aus Effizienzgründen allerdings erst die DMCA *safe harbor* prüfend: IO Group, Inc. v. Veoh Networks, Inc., 586 F.Supp.2d 1132 (N.D.Cal. 2008) („*Ordinarily, issues concerning liability would be examined before determining whether any safe harbor applies. [...] Under the circumstances presented here, the court finds it appropriate and more efficient to first address Veoh's motion as to the applicability of the safe harbor under DMCA section 512(c)"*); Costar Group, Inc. v. Loopnet, Inc. 164 F.Supp.2d 688, 699 (2001) („*[...] it is often appropriate for a court to decide issues out of the traditional order because a dispute of fact is only material if it can affect the outcome of a proceeding. Thus, to the extent, if at all, that LoopNet is entitled to summary judgment in its safe harbor defense, all other issues concerning damages liability for contributory infringement would be rendered immaterial"*); A.A. Hendrickson v. Ebay, Inc., 165 F. Supp. 2d 1082; 1132 (N.D.Cal. 2008).

[1085] H.R. Rep. 105-551(II), S. 50: „*[...] the limitations of liability apply if the provider is found to be liable under existing principles of law."*.

[1086] Bretan, 18 Berkeley Tech. L.J. 43, 62 (2003); Rasenberger/Pepe, 59 J. Copyright Soc'y U.S.A., 627, 658 (2012).

[1087] A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004 (9th Circ. 2001).

[1088] Ellison v. Robertson, 357 F.3d. 1072 (9th Cir. 2004).

[1089] Perfect 10, Inc. v. Cybernet Ventures, Inc., 213 F. Supp. 2d 1146 (2002).

[1090] Bretan, 18 Berkeley Tech. L.J. 43, 62 (2003).

[1091] Perfect 10, Inc. v. Cybernet Ventures, Inc., 213 F. Supp. 2d 1146, 1179 (2002).

Auch in Ellison v. Robertson, sah das Gericht Zweifel an einer angemessenen Umsetzung der *repeat infringer policy*.[1092]
Es ist reine Spekulation von *Bretan*, dass die Gerichte in den oben erwähnten Fällen zu einem anderen Ergebnis gelangt wären, wenn sie zuerst die Voraussetzungen des *safe harbor* geprüft hätten und anschließend eine Haftung nach den allgemeinen Haftungsregeln.
In der Literatur wird die Einordnung deshalb zu Recht vernachlässigt, da diese keine ersichtlichen praktischen Auswirkungen zur Folge hat.
Unstrittig ist hingegen die Anwendung eines zweistufigen Prüfungsmodells im Sinne einer gesonderten Prüfung der jeweiligen Privilegierung und der jeweils einschlägigen Haftungsnorm.[1093]

5. Einzelne Privilegierungstatbestände

Um in den Genuss der *safe harbor* des DMCA zu gelangen, hat der ISP gewisse Kriterien zu erfüllen. Diese variieren je nach Tätigkeitsbereich und basieren auf einem abgestuften Haftungssystem. Das Gesetz unterscheidet insgesamt vier verschiedene Bereiche, (1) *Transitory Digital Network Communications* (im Folgenden „Access-Provider" genannt), § 512 (a) DMCA, (2) *System Caching* (im Folgenden „Cache Provider" genannt), § 512 (b) DMCA, (3) *Information Residing on Systems or Networks At Direction of Users* (im Folgenden „Host-Provider" genannt), § 512 (c) DMCA und (4) *Information Location Tools*, § 512 (d) DMCA.

a) Allgemeine Voraussetzungen für eine Privilegierung

Neben den ISP-spezifischen Anspruchsvoraussetzungen, gibt es eine Reihe von allgemeinen Voraussetzungen, welche ein ISP

[1092] Ellison v. Robertson, 357 F.3d. 1072, 1082 (9th Cir. 2004).
[1093] S. Rep. 105-190, S. 19:*„Rather than embarking upon a wholesale clarification of these doctrines [contributory and vicarious liability, Anmerkung des Verfassers], the Committee decided to leave current law in its evolving state and, instead, to create a series of 'safe harbors', for certain common activities of service providers."*

erfüllen muss, um in den Genuss der Haftungsprivilegierung zu gelangen. Diese gelten gleichermaßen für alle ISP.

aa) Service Provider, § 512 (k) (1) DMCA

Zunächst muss der entsprechende ISP unter die Legaldefinition des Service Providers gem. § 512 (k) (1) DMCA fallen. Die genaue Bedeutung des Begriffs Service Providers ist davon abhängig, welchen der vier *safe harbors* der ISP für sich beansprucht. § 512 (k) (1) DMCA unterscheidet dahingehend, ob der ISP Schutz unter § 512 (a) DMCA oder unter §§ 512 (b) – (d) DMCA sucht.

(1) Service Provider gem.§ 512 (a) DMCA - Access-Provider

Handelt es sich um einen ISP, der den *safe harbor* von § 512 (a) DMCA sucht, so bedeutet der Begriff Service Provider gem. § 512 (k) (1) (A) DMCA *„an entity offering the transmission, routing, or providing of connections for digital online communications, between or among points specified by a user, of material of the user's choosing, without modification to the content of the material as sent or received"*. Diese Definition wurde abgeleitet aus der Definition des Begriffs *telecommunications* aus dem *Communications Act of 1934*[1094] und trägt der Tatsache Rechnung, dass es sich um *conduit-only functions* handelt, also um die bloße Durchleitung von Material.[1095]

Die Verbindungspunkte einer solchen Durchleitung müssen vom Nutzer ausgewählt werden. In *Columbia v. Fung*[1096] wurde dieses Kriterium verneint. Der Beklagte in diesem Fall unterhielt ein BitTorrent File Sharing-System. Dieses ermöglichte den Nutzern, in einem Datenbankindex durch die Eingabe bestimmter Schlagwörter nach Dateien zu suchen.[1097] Hatte der Nutzer die gewünschte Datei gefunden, konnte er diese in Form einer

[1094] 47 U.S.C. § 153 (50).
[1095] Siehe H.R. Rep. 105-551(II), S. 63; S. Rep. 105-190, S. 54.
[1096] Columbia Pictures Industries, Inc. v. Gary Fung, 710 F.3d 1020 (9th Cir. 2013).
[1097] Columbia Pictures Industries, Inc. v. Gary Fung, 710 F.3d 1020, 1028 (9th Cir. 2013).

Torrrent-Datei herunterladen.[1098] Öffnete er diese anschließend mit dem BitTorrent Programm, las das Programm die Informationen der Torrent-Datei und kontaktierte daraufhin den darin enthaltenen sog. *Tracker*.[1099] Der *Tracker* suchte daraufhin nach verfügbaren Peers, welche die gewünschte Datei zum Download bereithielten.[1100] Anschließend übermittelte er die entsprechende Adresse des Peers an das BitTorrent Programm des Nutzers, welches den Peer kontaktierte und mit dem Download der Datei begann.[1101]

Das Gericht verneinte die Anwendbarkeit der *safe harbor* Privilegien, da es sich bei dem Beklagten nicht um einen Service Provider im Sinne des § 512 (k) (1) (A) DMCA handele. Nicht der Nutzer wähle die Peers aus, von denen er eine bestimmte Datei herunterladen wolle, sondern die *Tracker* identifizierten und vermittelten dem Nutzer die verfügbaren Peers, welche die Datei zum Download bereithielten.[1102]

Unklar ist, ob der Begriff des Service Providers in diesem Sinne auch Einzelpersonen einschließt, da der Gesetzestext von einer *entity*[1103] spricht.[1104] Von Bedeutung ist dies insbesondere im Hinblick auf die Haftung für die Bereitstellung offener WLAN-Netze durch Privatpersonen.[1105] In der Rechtsprechung und im Schrifttum wurde diese Frage bislang nicht behandelt. Es ist jedoch davon auszugehen, dass auch Einzelpersonen unter die Privilegierung des § 512 (a) DMCA fallen. Es ist nicht ersichtlich, warum der *safe habor* für Access-Provider lediglich greifen sollte, sofern Unternehmen den Zugang vermitteln, in den Fällen des §§

[1098] Columbia Pictures Industries, Inc. v. Gary Fung, 710 F.3d 1020, 1028 (9th Cir. 2013).
[1099] Columbia Pictures Industries, Inc. v. Gary Fung, 710 F.3d 1020, 1028 (9th Cir. 2013).
[1100] Columbia Pictures Industries, Inc. v. Gary Fung, 710 F.3d 1020, 1028 (9th Cir. 2013).
[1101] Columbia Pictures Industries, Inc. v. Gary Fung, 710 F.3d 1020, 1028 (9th Cir. 2013).
[1102] Columbia Pictures Industries, Inc. v. Gary Fung, 710 F.3d 1020, 1041 (9th Cir. 2013).
[1103] Englisch für Rechtsträger, juristische Person.
[1104] Dies eher verneinend: Ballon, E-Commerce & Internet Law (2014-2015 Update), 4.12[2].
[1105] Siehe hierzu S. 323.

512 (b) – 512 (d) DMCA hingegen auch Einzelpersonen als Anbieter der Dienste erfasst sind.[1106]

(2) Service Provider gem. § 512 (b) – (d) DMCA

Sucht der ISP Schutz unter §§ 512 (b) – (d) DMCA, hat der Begriff des Service Providers gem. § 512 (k) (1) (B) DMCA die folgende Bedeutung: *„[...] a provider of online services or network access, or the operator of facilities therefor, and* [*the term service provider,* Anmerkung des Verfassers] *includes an entity described in subparagraph (A)"*.

Damit ist diese Definition wesentlich weiter als die des § 512 (k) (1) (A) DMCA. Umfasst sind sowohl Provider diverser Online-Dienste als auch solche Provider, die zusätzlich noch Dienste gem.§ 512 (k) (1) (A) DMCA erbringen.[1107]

Hierunter können bspw. Internet-Zugangsanbieter, E-Mail- und Chatroom-Anbeiter sowie Webseiten-Hosting-Anbieter fallen.[1108]

Auch die Rechtsprechung hat den Begriff des Service Providers gem. § 512 (k) (a) (B) DMCA sehr weit ausgelegt, so dass eine Vielzahl unterschiedlicher ISP hiervon erfasst werden.[1109]

bb) *Repeat Infringer Policy* § 512 (i) (1) (A) DMCA

Als weitere allgemeine Privilegierungsvoraussetzung muss der ISP eine Richtlinie (*policy*) festlegen, die es ihm erlaubt, Abonnenten und Kontoinhaber, die zum wiederholten Male Rechtsverletzungen begehen, von seinem Service auszuschließen. Zudem muss er die *policy* angemessen umsetzen und Abonnenten und Kontoinhaber über diese entsprechend informieren.

Aufgrund der Vielzahl unbestimmter Rechtsbegriffe in dieser Regelung[1110], ist die Auslegung der Gerichte zur näheren

---

[1106] So auch Stoltz, Victory for Open WiFi: Judge Rejects Copyright Troll's Bogus „Negligence" Theory.

[1107] H.R. Rep. 105-551(II), S. 64; S. Rep. 105-190, S. 54 f.

[1108] H.R. Rep. 105-551(II), S. 64; S. Rep. 105-190, S. 54 f.

[1109] Siehe bspw. In re Aimster Copyright Litigation, 252 F.Supp.2d 634, 658 (2002) (*„A plain reading of both definitions reveals that 'service provider' is defined so broadly that we have trouble imagining the existence of an online service that would not fall under the definitions, particularly the second"*).

[1110] „reasonably implemented", „appropriate circumstances", „repeat infringer".

Bestimmung der Voraussetzungen von entscheidender Bedeutung.[1111]

(1) Policy zum Ausschluss von Wiederholungstätern

Um diesem Kriterium gerecht zu werden, hat der ISP zunächst eine *policy* festzusetzen, die es ihm erlaubt, seine Nutzer unter bestimmten Umständen von seinem Dienst auszuschließen.

Es bedarf keiner detaillierten Beschreibung, wann und unter welchen Voraussetzungen der Nutzer von dem Dienst ausgeschlossen werden kann.[1112] Vielmehr ausreichend ist, dass diejenigen, welche wiederholt ihren Zugang zum Internet oder einem Dienst zur Nichtachtung von geistigen Eigentumsrechten Dritter missbrauchen, wissen, dass ein reales Risiko existiert, hierdurch diesen Zugang zu verlieren.[1113] Es wird von dem ISP nicht verlangt, dass er die Gründe für einen Ausschluss bereits im Vorhinein festlegt.[1114]

Um die Ernsthaftigkeit seiner *policy* zu untermauern, ist es dem ISP anzuraten, in dieser Urheberrechtsverletzungen explizit zu untersagen.[1115]

Umstritten ist jedoch wann genau ein Nutzer als Wiederholungstäter (*repeat infringer*) anzusehen ist und wann angemessene Umstände (*appropriate circumstances*) für seinen Ausschluss vorliegen. Das Gesetz enthält hierfür keine konkreten Bestimmungen. Schlüsse lassen sich aus dem *Senate* und *House Report* zum Gesetzesentwurf ziehen.

Hier ist zum einen ausdrücklich die Rede von Online-Urheberrechtsverletzungen.[1116] Zum anderen soll § 512 (i) (1) (A)

[1111] So auch Cooley, 64 SMU L. Rev. 691, 700 (2011).

[1112] Corbis Corp. v. Amazon.com, Inc., 351 F.Supp.2d 1090, 1100 (W.D. Wash. 2004).

[1113] Corbis Corp. v. Amazon.com, Inc., 351 F.Supp.2d 1090, 1101 (W.D. Wash. 2004); so auch H.R. Rep. 105-551(II), S. 61; S. Rep. 105-190, S. 52: *„However, those who repeatedly or fragrantly abuse their access to the Internet through disrespect for the intellectual property rights of others should know that there is a realistic threat of losing that access."*

[1114] Corbis Corp. v. Amazon.com, Inc., 351 F.Supp.2d 1090, 1101 (W.D.Wash. 2004).

[1115] Ballon, E-Commerce & Internet Law (2014-2015 Update), 4.12[2].

[1116] H.R. Rep. 105-551(II), S. 61; S. Rep. 105-190, S. 52, da beide Reports ausdrücklich von „repeat online infringers of copyright" und „on-line copyright

DMCA nicht den allgemeinen Grundsatz des § 512 (m) DMCA, dass der ISP keine Verpflichtung hat, seine Dienste zu überwachen oder aktiv nach Fakten zu suchen, welche auf eine verletzende Aktivität hinweisen, oder den Kenntnis-Standard gem. § 512 (c) DMCA untergraben.[1117] Der ISP hat keine Verpflichtung, potentielle Verletzungen zu suchen, seinen Dienst zu überwachen oder schwierige Beurteilungen dahingehend zu treffen, ob ein bestimmtes Verhalten eine Verletzung darstellt oder nicht.[1118] Vielmehr soll durch die gesetzliche Bestimmung sichergestellt werden, dass diejenigen, die zum wiederholten Male oder eklatant ihren Zugang nutzen, um Urheberrechte zu verletzen, von der Nutzung des Dienstes ausgeschlossen werden.[1119]

Der *District Court* in *Corbis v. Amazon* schließt daher folgerichtig darauf, dass der Kongress es dem ISP überlassen wollte, unter welchen Umständen er einen Nutzer ausschließt.[1120] Ihm stehe diesbezüglich eine gewisse Entscheidungsfreiheit zu. Untermauert würde diese Annahme auch durch die Tatsache, dass die vage und offene Sprache dieser Regelung im Gegensatz zu den sehr spezifischen Anforderungen an das *Notice and Takedown*-Verfahren in § 512 (c) DMCA stehe.[1121] Hätte der Kongress die Absicht gehabt, diesbezüglich genaue Anforderungen im Vorhinein festzulegen, so hätte er diese entsprechend im Gesetz konkret implementieren können.[1122]

Als Faustregel lässt sich jedenfalls für Host-Provider festhalten, dass alle Vorkommnisse, die den ISP nach § 512 (c) DMCA verpflichten, das streitgegenständliche Material zu entfernen oder

---

infringement“ sprechen, wird im Folgenden davon ausgegangen, dass der gesetzliche Begriff der „repeat infringers“ lediglich Urheberrechtsverletzungen umfasst, ausführlicher hierzu: Nimmer, Copyright Illuminated, S. 271 f.

[1117] H.R. Rep. 105-551(II), S. 61; S. Rep. 105-190, S. 52.

[1118] H.R. Rep. 105-551(II), S. 61; S. Rep. 105-190, S. 52.

[1119] H.R. Rep. 105-551(II), S. 61; S. Rep. 105-190, S. 52.

[1120] Corbis Corp. v. Amazon.com, Inc., 351 F.Supp.2d 1090, 1101 (W.D.Wash. 2004).

[1121] Corbis Corp. v. Amazon.com, Inc., 351 F.Supp.2d 1090, 1101 (W.D.Wash. 2004); zum Notice and Takedown-Verfahren siehe S. 296.

[1122] Corbis Corp. v. Amazon.com, Inc., 351 F.Supp.2d 1090, 1101 (W.D.Wash. 2004).

zu sperren, in die Bewertung, ob es sich um einen *repeat infringer* handelt, mit einbezogen werden sollten.[1123]

Aus diesem Grunde wird der Ausschluss eines Nutzers nach dem Erhalt von zwei bis drei *notifications* im Rahmen des *Notice and Takedown*-Verfahrens[1124], vorausgesetzt der Nutzer widerspricht diesen nicht im Wege einer sog. *counter notification*[1125], als angemessen angesehen werden können.[1126] Zusätzlich mit einbezogen werden sollten entsprechend auch Fälle, in denen der ISP aufgrund *actual knowledge*[1127] oder *red flag knowledge*[1128] Kenntnis von Urheberrechtsverletzungen erhält. Denn in sämtlichen der zuvor genannten Fälle trifft den Host-Provider auch eine gesetzliche Pflicht zur Entfernung bzw. Sperrung des Materials nach den Regelungen des DMCA.

Zurückzuweisen ist jedenfalls hinsichtlich des Host-Providers die Ansicht, dass grundsätzlich lediglich ein erfolgreiches Urheberrechtsverfahren gegen den Nutzer als Nachweis einer Urheberrechtsverletzung im Sinne des § 512 (i) (1) (A) DMCA anzusehen sei.[1129] Das im DMCA im Hinblick auf Host-Provider festgeschriebene *Notice and Takedown*-Verfahren ist gerade darauf ausgelegt, Gerichtsverfahren zu vermeiden und stattdessen die Rechte des Urhebers durch Kooperation mit dem ISP zu

---

[1123] So auch IO Group, Inc. v. Veoh Networks, Inc., 586 F. Supp.2d 1132, 1144 (N.D. Cal. 2008); White, 24 St. John's J. Legal Comment. 811, 824 (2010).

[1124] Siehe hierzu ausführlich S. 300.

[1125] Siehe hierzu ausführlich S. 333.

[1126] So im Ergebnis auch Capitol Records, LLC v. Vimeo, LLC, 972 F.Supp.2d 500, 513 (2013); Io Group, Inc. v. Veoh Networks, Inc. 586 F.Supp.2d 1132, 1143 (N.D. Cal. 2008); Ballon, E-Commerce & Internet Law (2014-2015 Update), 4.12[3][B][iii].

[1127] Siehe hierzu S. 269.

[1128] Siehe hierzu ausführlich S, 272, insbesondere auch der Problematik hinsichtlich der Bestimmung sog. red flags.

[1129] So aber bspw. Holznagel, GRUR Int 2007, 971,974; Nimmer, Copyright Illuminated, S. 281 mit dem Zusatz, dass hierzu auch Fälle zählen, in denen der ISP *actual knowledge* über eine Rechtsverletzung besitzt; ähnlich, allerdings nicht spezifisch eine rechtskräftige Verurteilung voraussetzend, aber doch „mehr" als reine *notifications*: Capitol Records, Inc. v. MP3Tunes LLC, 821 F.Supp.2d 627, 639 (S.D.N.Y. 2011) *„But takedown notices themselves are not evidence of blatant infringement and users could not be certain that they had downloaded infringing content [...] Thus, MP3tunes' decision to refrain from terminating those user accounts was appropriate."*; Corbis Corp. v. Amazon.com, Inc., 351 F.Supp.2d. 1090, 1105 (W.D.Wash. 2004); diesbezüglich ablehnend auch Ballon, Internet & E-Commerce (2014-2015 Update), 4.12[3][B][iii].

schützen.[1130] Für den Ausschluss von *repeat infringern* eine gerichtliche Verurteilung wegen Urheberrechtsverletzung zu verlangen, würde diesem Gedanken entgegenlaufen und den Rechteinhaber vor unverhältnismäßige Hürden stellen. Um die Rechte der Nutzer ausreichend zu achten, dürften allerdings nur solche *notifications* mit einbezogen werden, gegen die der vermeintliche Rechtsverletzer keinen Einspruch im Rahmen einer *counter notification* eingelegt hat.

Schwieriger ist die Beurteilung bei dem Access-Provider, da das Gesetz für diesen keine spezifische Konstruktion vorsieht, welche diesem eine Kenntnis von Urheberrechtsverletzungen seiner Nutzer zuschreibt. Den Access-Provider im Rahmen der Prüfung des § 512 (i) (1) (A) DMCA dem *Notice and Takedown*-Regime zu unterwerfen, würde dem gesetzgeberischen Modell entgegenlaufen, den verschiedenen ISP unterschiedliche Anspruchsvoraussetzungen für die Haftungsprivilegierung aufzuerlegen.[1131]

Welche genauen Kriterien zur Bestimmung eines *repeat infringers* im Falle des Access Providers heranzuziehen sind, wurde bislang gerichtlich noch nicht diskutiert. Denkbar wäre ein Ausschlussverfahren unter Bezug auf Benachrichtigungen über behauptete Rechtsverletzungen, die der Urheberrechtsinhaber im Rahmen des *Copyright Alert Systems*[1132] an den Access-Provider sendet (*notices of alleged infringement*). Allerdings würde dies im Widerspruch zur Struktur des DMCA stehen, welcher unterscheidet zwischen Host-Providern auf der einen Seite sowie Access-Providern, welche keinerlei Einflussnahme auf bzw. Kenntnis über die Inhalte haben, die ihre Nutzer durch ihre Netzwerke leiten und entsprechend für eine Privilegierung anderen Anspruchsvoraussetzungen unterliegen, auf der anderen Seite.[1133] Der Access-Provider Provider wurde absichtlich nicht dem *Notice-and Takedown*-Regime des § 512 (c) DMCA unterworfen.

[1130] Ballon, E-Commerce & Internet Law (2014-2015 Update), 4.12[3][B][iii].
[1131] Bridy, 89 Or. L. Rev. 81, 94 (2010), welche „*something more*" verlangt, aber nicht weiter ausführt, was genau sie unter „*something more*" versteht.
[1132] Siehe hierzu näher unter S. 387.
[1133] So auch Bridy, 89 Or. L. Rev. 81, 96 (2010).

Daher sollte sich auch die Bewertung des *repeat infringers* im Falle des Access-Providers, an den gesetzlichen Bestimmungen des § 512 (a) DMCA und nicht des 512 (c) DMCA orientieren. Sofern der Access-Provider demnach ohne jegliche Beeinflussung, Änderung, dauerhafter Speicherung oder Auswahl des Materials tätig wird, ist er nach dem DMCA zu privilegieren. Entsprechend sollte es auch einer gerichtlichen Verfügung bedürfen, um dem Nutzer eine Urheberrechtsverletzung im Sinne des § 512 (i) (1) (A) DMCA anzulasten und in die Bewertung des *repeat infringers* einzubeziehen.

Der ISP hat den *repeat infringer* zudem nur in *appropriate circumstances* auszuschließen. Was genau das heißt, ist unklar. Auch die Gerichte haben eine genaue Auseinandersetzung mit diesem Begriff bislang vermieden.[1134] *Nimmer* schlägt, gestützt auf die Gesetzesbegründung des *House* und *Senate Reports*, vor, die Bewertung der Angemessenheit darauf zu stützen, ob die jeweiligen Rechtsverletzungen vorsätzlich und gewerblich oder versehentlich und nicht vorsätzlich herbeigeführt wurden.[1135] Bei letzteren Rechtsverletzungen müssten die Nutzer nicht ausgeschlossen werden.[1136]

Der Ausschluss von Nutzern würde somit weitgehend ins Ermessen des ISP gestellt. Dies dürfte zwar nicht zu deren Rechtssicherheit beitragen, würde ihnen allerdings einen gewissen Handlungsspielraum bei der Beurteilung einräumen, was aufgrund fehlender konkreter gesetzlicher Vorgaben im Interesse des Gesetzgebers liegen dürfte.

[1134] In IO Group, Inc. v. Veoh Networks, Inc. (586 F.Supp.2d 1132) führt das Gericht lediglich wie folgt aus: *„A service provider reasonably implements its repeat infringer policy if it terminates users 'when appropriate'. [...] Section 512(i) itself does not clarify when it is 'appropriate' for service providers to act. It only requires that a service provider terminate users who are 'repeat infringers'."* Damit nutzt das Gericht den unbestimmten Begriff „appropriate" um damit den unbestimmten Terminus „resonably implements" zu definieren und nutzt anschließend den ebenfalls unbestimmten Begriff des „repeat infringers" um diejenigen Fälle zu bestimmen, die „appropriate" sind.

[1135] Nimmer, Copyright Illuminated, S. 294; siehe auch H.R. Rep. 105-551(II), S. 61; S. Rep. 105-190, S. 52: *„The Committee recognizes that there are different degrees of on-line copyright infringement, from the inadvertent and noncommercial, to the willful and commercial."*

[1136] Nimmer, Copyright Illuminated, S. 294.

Offen bleibt dennoch die Frage, inwiefern der ISP die Bewertung, ob eine behauptete Rechtsverletzung versehentlich oder aber vorsätzlich vorgenommen wurde, überhaupt vornehmen kann.

Letzten Endes ist davon auszugehen, dass den ISP keine starre Pflicht zum Ausschluss der Nutzer trifft. Ihm steht aufgrund der unbestimmten Rechtsbegriffe (*repeat infringer, appropriate circumstances*) sowohl hinsichtlich der Zahl der von ihm geforderten Rechtsverletzungen als auch der Art der Rechtsverletzungen immer noch ein gewisser Handlungsspielraum zu.

Dies ist auch Einklang mit den Gesetzgebungsmaterialien, nach denen es dem Gesetzgeber vorrangig darauf angekommen zu sein scheint, gegenüber den Nutzern der Dienste eine Abschreckwirkung zu entfalten.[1137]

(2) Angemessene Umsetzung

Der ISP hat die *policy* zudem angemessen umzusetzen (*reasonable implementation*), damit er nicht von dem *safe harbor*-Privileg ausgeschlossen wird. Wann eine angemessene Umsetzung vorliegt, ist fraglich.

In *Perfect 10 v. CCBill* hat der *Ninth Circuit Court of Appeals* ausgeführt, dass eine Umsetzung vorliegt, wenn der ISP über ein funktionierendes Benachrichtigungssystem bzgl. der *notifications* verfügt, er ein Verfahren hat, mit diesen *notifications* umzugehen und er den Urheber nicht aktiv davon abhält, Informationen zu sammeln, die für die *notification* von Nöten sind.[1138]

Dieser Interpretation wird jedoch entgegengehalten, dass eine Beurteilung der Umsetzung nicht auf die Beziehung zwischen ISP und Urheberrechtsinhaber gerichtet sein sollte, sondern zwischen ISP und Nutzer.[1139] Die Beziehung zwischen ISP und

---

[1137] H.R. Rep. 105-551(II), S. 61; S. Rep. 105-190, S. 52: *„[...] those who repeatedly or flagrantly abuse their access to the Internet [...] should know that there is a realistic threat of losing that access"*.

[1138] Perfect 10, Inc. v. CCBill LLC, 488 F.3d 1102, 1109 (9th Cir. 2007); Capitol Records, Inc. v. MP3Tunes, LLC, 821 F.Supp.2d 627, 637 (S.D.N.Y. 2011).

[1139] Ludwig, Boston College Intellectual Property & Technology Forum, 8 (2006).

Urheberrechtsinhaber wird bereits in den sorgfältig ausgearbeiteten Bestimmungen zum *Notice and Takedown*-Verfahren geregelt, welche detailliert das Kommunikationsverfahren zwischen diesen beiden Parteien regelt.[1140]

Zudem birgt die unterschiedlose Prüfung gemäß der vom *Ninth Circuit* entwickelten Kriterien die Gefahr, einzelfallabhängige Faktoren sowie den tatsächlichen Wortlaut des Gesetzestextes unberücksichtigt zu lassen.[1141]

Als sicher gilt jedenfalls, dass *reasonableness* keine 100-%ige Präzision voraussetzt, es wird keine perfekte Umsetzung verlangt.[1142]

Der *Ninth Circuit* sowie einige weitere Gerichte haben zudem im Rahmen einer negativen Abgrenzung ausgeführt, dass die *policy* jedenfalls als unangemessen (*unreasonable*) anzusehen sei, wenn der ISP es verfehlt, einen Nutzer, welcher als *repeat infringer* auffällig wird, auszuschließen, obwohl er Kenntnis von dessen Rechtsverletzung hat.[1143]

An diese negative Abgrenzung sollte auch die Leseart des Begriffs *reasonably implemented* anknüpfen und sich nicht an der korrekten Implementierung des *Notice and Takedown*-Verfahrens, sondern vielmehr an der ordnungsgemäßen Umsetzung der *Policy* im Hinblick auf den Ausschluss des Nutzers als *repeat infringer* orientieren.[1144]

Dieser Ansatz wird auch dem Wortlaut der Vorschrift gerecht. Eine angemessene Umsetzung bedeutet nicht mehr, als dass dem Wiederholungstäter tatsächlich der Anschluss gekündigt bzw. er

---

[1140] Ludwig, Boston College Intellectual Property & Technology Forum, 8 (2006).

[1141] Ballon, E-Commerce & Internet Law (2014-2015 Update), 4.12[3][B][iv].

[1142] Io Group, Inc. v. Veoh Networks, Inc., 586 F.Supp.2d 1132, 1144 (N.D.Cal. 2008); Ballon, E-Commerce & Internet Law (2014-2015 Update), 4.12[3][B][iv].

[1143] Perfect 10, Inc. v. CCBill LLC, 488 F.3d 1102, 1111 (9th Cir. 2007); Io Group, Inc. v. Veoh Networks, Inc., 586 F.Supp.2d 1132, 1145 (N.D.Cal. 2008); Capitol Records, Inc. v. MP3Tunes, LLC., 821 F.Supp.2d 627, 637 (S.D.N.Y. 2011).

[1144] So im Ergebnis auch Corbis Corp. v. Amazon.com, Inc., 351 F.Supp.2d 1090, 1104 (W.D.Wash. 2004), allerdings mit dem Zusatz, dass es sich um Kenntnis über „*user's blatant, repeat infringement of a willful and commercial nature*" handeln müsse.

von dem Dienst ausgeschlossen werden muss. In diesem Fall wird die *policy*, welche den Ausschluss der *repeat infringer* beschließt, angemessen umgesetzt.

(3) Benachrichtigung der Abonnenten/Kontoinhaber

Zu guter Letzt muss der ISP seine Abonnenten (*subscriber*) bzw. Kontoinhaber (*account holder*) über seine *policy* informieren. Dieses Kriterium lässt sich einfach durch einen Link auf der Webseite des ISP verwirklichen.[1145] Eine ausdrückliche Zustimmung des *subscribers/account holders* wird nicht verlangt.[1146]

(4) Anwendbarkeit auf ISP ohne Abonnenten/Kontoinhaber

Unklar ist, warum der Kongress sich bei dieser Bestimmung für den Wortlaut der *subscriber* und *account holder* entschieden hat und nicht, wie an anderer Stelle des DMCA, lediglich des *user*.

Teilweise wird die Auffassung vertreten, dass aufgrund des Wortlauts der Vorschrift, ISP, die keine *subscriber* oder *account holder* haben, sondern lediglich Nutzer/Webseitenbesucher, aus dem Anwendungsbereich des § 512 (i) (1) (A) DMCA herausfallen.[1147] Dazu würden beispielsweise *Information Location Tools* oder einfache Webseiten zählen, sofern hier keine Art von vertraglicher Beziehung zwischen Nutzer und ISP besteht.[1148]

In den *Senate* und *House Reports* wird hinsichtlich des Begriffs des *subscribers* ausgeführt, dass der Begriff der *subscriber „include[s] account holders that have a business relationship with the service provider that justifies treating them as subscribers [...], even if no formal subscription agreement exists. For example, „subscribers" would include students who are granted access to a university's system or network for digital on-line communications; employees who have access to their employer's system or network; or household members with access to a consumer on-line service by*

[1145] Nimmer, Copyright Illuminated, S. 296; Ballon, E-Commerce & Internet Law (2014-2015 Update), 4.12[3][B][ii].
[1146] Nimmer, Copyright Illuminated, S. 296.
[1147] E-Commerce & Internet Law (2014-2015 Update), 4.12[3][B][ii].
[1148] E-Commerce & Internet Law (2014-2015 Update), 4.12[3][B][ii].

virtue of a subscription agreement between the service provider and another member of that household.“[1149]

Hieraus lassen sich keine klaren Schlüsse bezüglich Diensten ziehen, bei denen Nutzer weder über ein Abonnement noch ein Konto verfügen sowie über keinerlei Geschäftsbeziehung zu dem ISP. Gerichte haben sich mit dem genauen Ausmaß des Begriffes bislang noch nicht beschäftigt.

Grundsätzlich sind drei Interpretationen denkbar. Zum einen wäre es möglich, dass ISP, welche weder über Abonnenten noch über Kontoinhaber verfügen, diese initiale Zulässigkeitsvoraussetzung der *safe harbor*-Bestimmungen nicht erfüllen können und somit von vornherein aus dem Schutzbereich herausfallen.[1150] Es ist allerdings unwahrscheinlich, dass dies im Sinne des Gesetzgebers ist, da hierdurch jegliche *Information Location Tools* automatisch nicht unter die DMCA *safe harbor*-Bestimmungen fallen würden. Die Gesetzgebungsgeschichte sowie die expliziten Aufnahme der *Information Location Tools* in § 512 (d) DMCA sprechen gegen eine entsprechende Interpretation.

Nach einer anderen Interpretation könnte es sich schlicht um einen Fehler des Kongresses während der Ausarbeitung der DMCA-Bestimmungen handeln.[1151] Es ist allerdings unwahrscheinlich, dass der Kongress die drei verschiedenen Begriffe der *user*, *subscriber* und *account holder* gewählt hat, wenn er eigentlich bei allen drei dieser Begriffe das gleiche ausdrücken wollte.

Es ist daher der dritten Interpretation zuzustimmen, wonach der Kongress absichtlich nicht den Begriff der Nutzer verwendet, um solche ISP, die über keine Abonnenten oder Kontoinhaber

---

[1149] H.R. Rep. 105-551(II), S. 61 Fn. 3; S. Rep. 105-190, S. 52, Fn. 24.

[1150] Walker, Virginia Journal of Law & Technology Vol. 9, No.2, para. 40 (2004), der eine entsprechende Interpretation allerdings wegen des unerwünschten Effekts auf die Service Provider, die am wenigsten von Urheberrechtsverletzungen profitieren, ablehnt.

[1151] So auch Walker, Virginia Journal of Law & Technology Vol. 9, No.2, para. 45 (2004), der in einem solchen Fall den Kongress dazu aufruft, das Gesetz entsprechend zu ändern bzw. für den Fall, dass dieser keine Änderung des Gesetzes vornimmt, die Gerichte dazu anhält, diese Bestimmung großzügig auszulegen und auf sämtliche ISP zu erstrecken, auch wenn diese keine *subscriber* oder *account holder* haben.

verfügen, von der Voraussetzung des § 512 (i) (1) (A) DMCA zu befreien.[1152]

Aufgrund der einfachen Einrichtung und Umsetzung sowie der unsicheren Rechtslage hinsichtlich dieser Bestimmung, wird teils auch diesen ISP dazu geraten, eine entsprechende *policy* zu implementieren.[1153] Verkannt wird hierbei allerdings, dass zwar eine formale *policy* ohne Probleme auf der Webseite angebracht werden kann, dass jedoch die Umsetzung, wie beispielsweise der tatsächliche Ausschluss eines Nutzers, bei einer allgemein zugänglichen Suchmaschine, schlicht nicht möglich ist.

cc) Standard Technical Measures

Um den Schutz der DMCA *safe harbor* in Anspruch zu nehmen, hat der ISP gem. § 512 (1) (B) DMCA zudem technischen Standardmaßnahmen (*standard technical measures*) Rechnung zu tragen und darf diese nicht beeinträchtigen.

Gemäß der Legaldefinition des Begriffs der *standard technical measures* werden hierunter technische Maßnahmen verstanden, die von Urheberrechtsinhabern genutzt werden, um ihre geschützten Urheberrechtswerke zu identifizieren und schützen[1154]. Zudem müssen diese *standard technical measures* in einem offenen, fairen, freiwilligen und branchenübergreifendem Standardprozess mit einem breiten Konsens zwischen Urheberrechtsinhabern und ISP entwickelt worden[1155], für jede Person zu vernünftigen und nicht diskriminierenden Konditionen verfügbar sein[1156] und keine substantiellen Kosten für den ISP oder Belastungen seines Systems oder Netzwerkes verursachen[1157].

[1152] So auch Walker, Virginia Journal of Law & Technology Vol. 9, No.2, para. 44.

[1153] E-Commerce & Internet Law (2014-2015 Update), 4.12[3][B][ii]; viele große Suchmaschinen-Anbieter haben eine entsprechende *policy* implementiert, z.B. Google, einsehbar unter http://www.google.com/dmca.html, zuletzt besucht am 24.04.2016.

[1154] § 512 (2) DMCA.

[1155] § 512 (2) (A) DMCA.

[1156] § 512 (2) (B) DMCA.

[1157] § 512 (2) (C) DMCA.

Es ist unklar, ob derzeit überhaupt eine Technologie existiert, welche eine *standard technical measure* darstellt.[1158] Senat und Repräsentantenhaus sind in ihren *Reports* noch davon ausgegangen, dass sog. *recognized open standard bodies* bzw. *ad hoc groups* einen entsprechenden Standard entwickeln.[1159] Dies ist, soweit ersichtlich, bislang allerdings nicht geschehen.[1160] Auch Gerichte haben sich nur äußerst zurückhaltend zu dieser Bestimmung geäußert.

In *Perfect 10 v. CCBill* hat der *Court of Ninth Circuit* lediglich ausgeführt, dass der Begriff der *standard technical measures* sich auf eine eng begrenzte Gruppe von Technologie-Lösungen für Online-Urheberrechtsverletzungen beziehe.[1161] Es bestehe jedenfalls keine pro-aktive Pflicht der ISP *standard technical measures* einzusetzen.[1162] Der ISP hat diese lediglich passiv zu tolerieren und sein System bzw. Netzwerk so zu unterhalten, dass es mit diesen kompatibel ist.[1163]

Da bislang keine Einigung zwischen ISP und Urheberrechtsinhaber bzgl. der *standard technical measures* zustande gekommen ist, wird diese Voraussetzung aller Voraussicht nach auch in naher Zukunft keine Rolle in der Praxis darstellen. Bei Fehlen von *standard technical measures*, kann der ISP diesen auch keine Rechnung tragen.

dd) Protection of Privacy

Zu den allgemeinen Privilegierungsvoraussetzungen zählt auch der Schutz der Privatsphäre der Internetnutzer. Entsprechend bestimmt § 512 (m) (1) DMCA, dass den ISP keine Verpflichtung trifft, seinen Dienst zu überwachen oder aktiv nach Tatsachen zu suchen,

---

[1158] E-Commerce & Internet Law (2014-2015 Update), 4.12[3][C].
[1159] H.R. Rep. 105-551(II), S. 61; S. Rep. 105-190, S. 52.
[1160] E-Commerce & Internet Law (2014-2015 Update), 4.12[3][C]; Gallo, 34 Colum. J.L. & Arts 283, 300 (2011).
[1161] Perfect 10, Inc. v. CCBill LLC, 488 F.3d 1102, 1115 (9th Cir. 2007).
[1162] Gallo, 34 Colum. J.L. & Arts 283, 302 (2011); diese Ansicht wird auch gestützt durch den Wortlaut des § 512 (i) (2) DMCA, welcher von „*technical measures that are used by copyright owners to identify and protect copyrighted works" spricht und nicht von „technical measures that are used by the service provider*".
[1163] Gallo, 34 Colum. J.L. & Arts 283, 302 (2011).

die auf eine rechtsverletzende Tätigkeit hinweisen. Als Einschränkung verweist die Bestimmung auf die *standard technical measures*, die der ISP zu beachten hat.

Nimmer weist daher auf die theoretische Möglichkeit hin, dass sofern in der Zukunft *standard technical measures* im Sinne des § 512 (i) (B) DMCA auftauchen, die eine Überwachung voraussetzen, auch der ISP entsprechend zu einer Überwachung in diesem Umfang verpflichtet sei.[1164] Dass dies tatsächlich geschehen wird, hält er allerdings für nicht wahrscheinlich.[1165]

Dem ISP steht es jedoch frei, seinen Dienst freiwillig zu überwachen.[1166] Durch solch freiwillige Maßnahmen darf dem ISP entsprechend nicht der Schutz des *safe harbor* verloren gehen.[1167]

Zudem obliegt der ISP gem. § 512 (m) (2) DMCA keiner Verpflichtung, Zugang zu Material zu gewähren, dieses zu entfernen oder den Zugang hierzu zu sperren in Fällen, in denen eine solche Handlung durch Gesetz untersagt ist. Als Beispiel nennen die Gesetzgebungsmaterialien den *Electronic Communications Privacy Act*.[1168]

Durch diese Bestimmung soll sichergestellt werden, dass der ISP keine anderen Gesetze verletzen muss, um Urheberrechte zu schützen.[1169] Der ISP wird daher auch dann privilegiert, wenn er die Entfernung oder Sperrung von Material verweigert, diese Verweigerung aber darauf beruht, dass eine entsprechende Entfernung bzw. Sperrung aufgrund eines anderen Gesetzes verboten ist.[1170]

Des Weiteren könnten die Gerichte nach *Nimmer* auch die Überschrift des § 512 (m) DMCA „Protection of Privacy“ als grundsätzliches Ziel dieser Regelung berücksichtigen.[1171]

[1164] Nimmer on Copyright, § 12B.02 [B] [3] [b].
[1165] Nimmer on Copyright, § 12B.02 [B] [3] [b].
[1166] Conference Report, S. 73.
[1167] Conference Report, S. 73.
[1168] H.R. Rep. 105-551(II), S. 65; S. Rep. 105-190, S. 55.
[1169] Nimmer on Copyright, § 12B.02 [B] [3] [b].
[1170] Nimmer on Copyright, § 12B.02 [B] [3] [b].
[1171] Nimmer on Copyright, § 12B.02 [B] [3] [b].

b) Host-Provider

Die Haftungsprivilegierung des Host-Providers ist in § 512 (c) DMCA geregelt. Neben den allgemeinen Voraussetzungen zur Inanspruchnahme des *safe harbor*-Privilegs, welche alle ISP gleichermaßen erfüllen müssen, hat der Host-Provider zusätzlich die nachfolgenden provider-spezifischen Voraussetzungen zu erfüllen.

Dieser ist nicht verantwortlich für Urheberrechtsverletzungen *„by reason of the storage at the direction of a user of material that resides on a system or network controlled or operated by or for the service provider“*, sofern er die Voraussetzungen nach § 512 (c) (A) - (C) DMCA erfüllt.

Die Privilegierung erstreckt sich auch auf die Mitarbeiter des Host-Providers.[1172]

aa) Speicherung auf Anweisung des Nutzers

Das Material muss vom Host-Provider auf Anweisung des Nutzers (*at the direction of the user*) gespeichert worden sein. Dies ist nicht der Fall, wenn sich das Material aufgrund eigener Handlung oder Entscheidung des Host-Providers auf dessen Plattform befindet.[1173]

Unbeachtlich ist allerdings, ob der Host-Provider die hochgeladene Datei automatisch in ein anderes Format konvertiert[1174] oder seine Mitarbeiter das Material vor dem Upload sichten und auf offensichtliche Rechtswidrigkeiten hin überprüfen[1175].

Denn auch in diesen Fällen wurde das Material auf Anweisung des Nutzers hin hochgeladen. Dass das Material in der Folge durch den Host-Provider in einem automatischen Prozess in ein einheitliches Format umgewandelt wird, da die Mehrzahl der Internetnutzer über Software verfügt, die dieses Format abspielen kann, ist für die Bestimmung auf wessen Veranlassung das Material gespeichert

---

[1172] Hendrickson v. Ebay, Inc., 165 F. Supp. 2d 1082, 1094 f.:*„To hold that the safe harbor provision of the DMCA protects the company but not its employees for the same alleged bad acts would produce an absurd result.“*

[1173] H.R. Rep. 105-551(II), S. 53; S. Rep. 105-190, S. 43.

[1174] Io Group, Inc. v. Veoh Networks, Inc., 586 F.Supp.2d 1132, 1148 (N.D.Cal. 2008).

[1175] Costar Group, Inc. v. LoopNet, Inc., 164 F.Supp.2d 688, 702 (2001).

wurde, unbeachtlich.[1176] Von Bedeutung ist lediglich, dass der Nutzer den Upload ursprünglich initiiert hat.[1177]

Auch wenn das Material nach Upload des Nutzers durch Mitarbeiter des Host-Providers auf offensichtliche Rechtsverletzungen überprüft wird, bevor es online gestellt wird, bedeutet dies nicht, dass der Host-Provider in die Auswahl des Materials involviert ist.[1178] Der Host-Provider fungiere hier lediglich als *Gateway*.[1179]

Auch ist der Begriff des Speicherns weit auszulegen. § 512 (c) DMCA ist nicht lediglich auf Vorgänge, die das Speichern des Materials betreffen, beschränkt.[1180] In *UMG v. Shelter*[1181] stellte die Klägerin infrage, dass die automatischen Vorgänge während des Uploads eines Videos auf der Videoplattform Veoh, insbesondere die öffentliche Zugangsverschaffung zu dem Video, innerhalb des Bereichs des Speicherns fallen. Sie argumentierte, dass die Zugangsverschaffung zu dem Video über dessen Speicherung hinausginge.[1182] Deshalb fielen sowohl die Umwandlung der Videos in Flash-Files sowie das Streaming und der Download der Videos außerhalb des Anwendungsbereichs des § 512 (c) DMCA.[1183]

Der *Ninth Circuit* wies dies allerdings mit der Begründung zurück, dass diese Leseart zu restriktiv sei.[1184] Der Gesetzeswortlaut spreche nicht davon, dass die rechtsverletzende Handlung die Speicherung sein soll (*that infringing conduct be storage*), sondern lediglich dass diese aufgrund der Speicherung geschehe (*by reason*

[1176] Io Group, Inc. v. Veoh Networks, Inc., 586 F.Supp.2d 1132, 1148 (N.D.Cal. 2008).
[1177] Io Group, Inc. v. Veoh Networks, Inc., 586 F.Supp.2d 1132, 1148 (N.D.Cal. 2008).
[1178] Costar Group, Inc. v. LoopNet, Inc., 164 F.Supp.2d 688, 702 (2001).
[1179] Costar Group, Inc. v. LoopNet, Inc., 164 F.Supp.2d 688, 702 (2001).
[1180] Io Group, Inc. v. Veoh Networks, Inc., 586 F.Supp.2d 1132, 1147 (N.D.Cal. 2008).
[1181] UMG Recordings, Inc. v. Shelter Capital Partners LLC, 718 F.3d 1006 (9th Cir. 2013).
[1182] UMG Recordings, Inc. v. Shelter Capital Partners LLC, 718 F.3d 1006, 1016 (9th Cir. 2013).
[1183] UMG Recordings, Inc. v. Shelter Capital Partners LLC, 718 F.3d 1006, 1016 (9th Cir. 2013).
[1184] UMG Recordings, Inc. v. Shelter Capital Partners LLC, 718 F.3d 1006, 1016 (9th Cir. 2013).

of the storage).[1185] Damit solle sichtlich mehr erfasst werden als lediglich elektronische Online-Speicher.[1186]

Gestützt werde diese Rechtsauffassung auch durch die Tatsache, dass das Gesetz gerade voraussetzt, dass der Host-Provider Zugang zu dem von den Nutzern gespeicherten Inhalten herstellt.[1187] Denn nur durch die Zugangsvermittlung zu dem auf der Plattform des Host-Providers befindlichem Material kann der Urheberrechtsinhaber Kenntnis hiervon erlangen und den Host-Provider anschließend gem. des in § 512 (c) (3) DMCA geregelten *Notice and Takedown*-Verfahrens zur Löschung bzw. Sperrung des Zugangs auffordern.[1188]

Auch die Gesetzeshistorie führt als Beispiele für ein solches Speichern etwa das Zurverfügungstellen von Speicherplatz auf dem Server für eine Webseite des Nutzers, für einen Chatroom oder ein anderes Forum, in welchem die Nutzer Material posten können, auf.[1189]

Rasenberger/Pepe sehen diese Interpretation des Speicherns i.S.d. § 512 (c) DMCA als kritisch an.[1190] Sie halten es insbesondere für unwahrscheinlich, dass der Kongress eine Auslegung des Begriffs *by reason of storage* dahingehend beabsichtigt hatte, dass dieser auch Fälle von *filesharing* durch Filehosting-Dienste umfasst.[1191]

Dieser Auffassung ist dahingehend zuzustimmen, dass der Kongress bei der Ausarbeitung des Gesetzesentwurfs nicht eine solche Konstellation im Sinn hatte. Schließlich war zu dieser Zeit diese technische Entwicklung der verschiedenen Internet-Dienste, wie sie heute existieren, noch überhaupt nicht absehbar. Dies ändert jedoch nichts daran, dass der Begriff *by reason of storage* so auszulegen ist, dass er auch andere mit dem Speichern verbundene

[1185] UMG Recordings, Inc. v. Shelter Capital Partners LLC, 718 F.3d 1006, 1016 (9th Cir. 2013).
[1186] UMG Recordings, Inc. v. Shelter Capital Partners LLC, 718 F.3d 1006, 1016 (9th Cir. 2013).
[1187] UMG Recordings, Inc. v. Shelter Capital Partners LLC, 718 F.3d 1006, 1017 (9th Cir. 2013).
[1188] UMG Recordings, Inc. v. Shelter Capital Partners LLC, 718 F.3d 1006, 1018 (9th Cir. 2013).
[1189] H.R. Rep. 105-551(II), S. 53; S. Rep. 105-190, S. 43.
[1190] Rasenberger/Pepe, 59 J. Copyright Soc'y U.S.A., 627, 665 f. (2012).
[1191] Rasenberger/Pepe, 59 J. Copyright Soc'y U.S.A., 627, 666 (2012).

Vorgänge, wie die öffentliche Zugänglichmachung des Materials, umfasst. Eine solche Auslegung stimmt auch mit dem Sinn und Zweck der *safe harbor* Bestimmung des § 512 (c) DMCA überein. Zudem ist zu bedenken, dass ohne eine Zugangsverschaffung an die Nutzer bereits fraglich ist, ob es überhaupt zu einer Urheberrechtsverletzung kommt.

bb) Material auf dem System/Netzwerk des Host-Providers

Voraussetzung ist nicht, dass die Urheberrechtsverletzung auf dem rechtswidrigen Material basiert, sie kann auch durch eine rechtswidrige Handlung herbeigeführt worden sein.[1192] Dies ergibt sich bereits aus dem nachfolgenden § 512 (c) (1) (A) (i) DMCA, wo explizit von *„material or an activity using the material"* die Rede ist. Der *Ninth Circuit* führte diesbezüglich in *Columbia v. Fung* aus, dass *„§ 512 (c) explicitly covers not just the storage of infringing material, but also infringing ‚activit[ies]' that us[e] the material [stored] on the system or network."*.[1193]

Im Bereich der Urheberrechtsverletzungen ist dies von besonderer Bedeutung, da in der Regel nicht das Material an sich rechtswidrig ist, sondern die jeweilige Handlung durch den Nutzer, üblicherweise der Upload der Datei ohne entsprechende Lizenz oder Einwilligung des Rechteinhabers.

cc) Kenntnis und unverzügliches Tätigwerden

§ 512 (c) (A) DMCA enthält drei alternative Voraussetzungen, die der Host-Provider erfüllen muss, um die Haftungsprivilegierung in Anspruch nehmen zu können.

[1192] Columbia Pictures Industries, Inc. v. Gary Fung, 710 F.3d 1020, 1042 (9th Cir. 2013).

[1193] Columbia Pictures Industries, Inc. v. Gary Fung, 710 F.3d 1020, 1042 (9th Cir. 2013); siehe auch H.R. Rep. 105-551(II), S. 53; S. Rep. 105-190, S. 44 *„The term 'activity' is intended to mean activity using the material on the system or network. The Committee intends such activity to refer to wrongful activity that is occurring at the site on the provider's system or network at which the material resides, regardless of whether copyright infringement is technically deemed to occur at that site or at the location where the material is received. For example, the activity at an online site offering audio or video may be unauthorized public performance of a musical composition, a sound recording, or an audio-visual work, rather than (or in addition to) to creation of an unauthorized copy of these works."*

(1) Keine tatsächliche Kenntnis – No actual knowledge

Gemäß § 512 (c) (1) (A) (i) DMCA ist der Host-Provider privilegiert, sofern er keine tatsächliche Kenntnis (*actual knowledge*) von der Rechtsverletzung hat.

Nach h.M. ist der Begriff der *actual knowledge* im Sinne einer subjektiven tatsächlichen Kenntnis zu verstehen.[1194]

Fraglich ist allerdings, wann eine solche subjektive Kenntnis und damit *actual knowledge* vorliegt. Die Gesetzgebungsmaterialien sind hier wenig aufschlussreich. Zwar wird dort auf der einen Seite ausgeführt, dass der Host-Provider, sofern er von den Privilegien profitieren möchte, das rechtsverletzende Material herunternehmen bzw. sperren muss, sobald er Kenntnis im Sinne des DMCA hat, auch wenn der Urheberrechtsinhaber keine entsprechende *notification* sendet.[1195] Auf der anderen Seite wird hervorgehoben, dass dem Host-Provider kein *actual knowledge* aufgrund von Informationen zugerechnet werden kann, die der Urheberrechtsinhaber dem Host-Provider mitteilt, sofern diese nicht den Anforderungen einer *notification* entsprechen.[1196]

Unklar bleibt, welche Fälle der Gesetzgeber im Sinn hatte, die den Host-Provider dazu verpflichten, ohne entsprechende *notification* das Material herunterzunehmen bzw. zu sperren.

Die wohl h.M. der Rechtsprechung geht davon aus, dass *actual knowledge* lediglich durch eine DMCA-konforme *notification* erlangt werden kann.[1197] Daher nimmt ein Teil des Schrifttums an, dass es unwahrscheinlich sei, dass ein Gericht *actual knowledge*

[1194] Columbia Pictures Industries, Inc. v. Fung, 710 F.3d 1020, 1043 (9th Cir. 2013); UMG Recordings, Inc. v. Shelter Capital Partners, 718 F.3d 1006, 1026 (9th Cir. 2013); Viacom Intern., Inc. v. YouTube, Inc., 676 F.3d 19, 31 (2nd Cir. 2012); Reese, 34 Sw. U. L. Rev. 287, 299 (2004).

[1195] H.R. Rep. 105-551(II), S. 54; S. Rep. 105-190, S. 45.

[1196] H.R. Rep. 105-551(II), S. 54; S. Rep. 105-190, S. 45; siehe auch § 512 (c) (3) (B) (i) DMCA.

[1197] So bspw. UMG Recordings, Inc. v. Shelter Capital Partners, 718 F.3d 1006, 1025 (9th Cir. 2013); Io Group, Inc. v. Veoh Networks, Inc., 586 F.Supp.2d 1132, 1148 (N.D.Cal. 2008); Corbis Corporation v. Amazon.com, Inc., 351 F.Supp.2d 1090, 1107 (W.D.Wash. 2004); Sirichit, 23 Alb. L. J. Sci. & Tech. 85, 128 (2013).

eines Host-Providers bejahe, ohne dass dieser zuvor eine *notification* erhalten habe.[1198]

Der *Second Circuit* scheint jedoch auch andere Wege für möglich zu halten, auf denen der Host-Provider *actual knowledge* erlangen kann.[1199] Das Gericht führt aus, dass *actual knowledge* im Sinne einer subjektiven Kenntnis einer Rechtsverletzung zu verstehen sei.[1200] Es sei daher möglich, dass der Host-Provider durch eigene betriebsintern generierte Kenntnis eine *actual knowledge* i.S.d. § 512 (c) DMCA über eine spezifische Rechtsverletzung erlangt hat.[1201]

Dem *Second Circuit* ist hier zuzustimmen. *Actual knowledge* ist nach h.M. als subjektive Kenntnis zu verstehen. Es wäre widersinnig eine subjektive Kenntnis lediglich aufgrund des vorherigen Empfangs einer *notification* zu bejahen.[1202] Dies ergibt sich bereits daraus, dass das *Notice and Takedown*-Verfahren unabhängig von § 512 (c) (1) (A) DMCA in § 512 (c) (1) (C) DMCA geregelt wurde.[1203] Würden unter den Begriff der *actual knowledge* nur solche Fälle fallen, in denen der Host-Provider zuvor eine *notification* erhalten hat, hätte es einer separaten Regelung für die *actual knowledge* erst gar nicht bedurft.[1204] Das *Notice and Takedown*-Verfahren des § 512 (c) (1) (C) DMCA, welches vom Erhalt einer *notification* abhängig gemacht wurde, dient lediglich dazu, dem Host-Provider aufgrund gesetzlicher Bestimmung eine Kenntnis zuzuschreiben, sofern der Rechteinhaber eine den formellen Anforderungen entsprechende *notification* sendet. Dadurch ist aber gerade nicht zugleich sichergestellt, dass es sich tatsächlich um

[1198] Sirichit, 23 Alb. L. J. Sci. & Tech. 85, 130 (2013).
[1199] Viacom Intern., Inc. v. YouTube, Inc., 676 F.3d 19, 34 (2nd Cir. 2012); so auch Rasenberger/Pepe, 59 J. Copyright Soc'y U.S.A., 627, 676 (2012).
[1200] Viacom Intern., Inc. v. YouTube, Inc., 676 F.3d 19, 31 (2nd Cir. 2012).
[1201] Viacom Intern., Inc. v. YouTube, Inc., 676 F.3d 19, 34 (2nd Cir. 2012); so auch Rasenberger/Pepe, 59 J. Copyright Soc'y U.S.A., 627, 676 f. (2012).
[1202] So im Ergebnis auch Rasenberger/Pepe, 59 J. Copyright Soc'y U.S.A., 627, 689 f. (2012).
[1203] So auch Rasenberger/Pepe, 59 J. Copyright Soc'y U.S.A., 627, 689 (2012).
[1204] So auch Rasenberger/Pepe, 59 J. Copyright Soc'y U.S.A., 627, 689 (2012).

urheberrechtsverletzendes Material handelt. Es wird hierdurch vielmehr die gesetzliche Fiktion einer Rechtsverletzung geschaffen. Bei einer Kenntnis im subjektiven Sinne ist aber vielmehr erforderlich, dass der Host-Provider tatsächliche Kenntnis über die Rechtswidrigkeit eines spezifischen Materials hat.[1205] Daher vermittelt auch eine *notification* an den Host-Provider nicht unbedingt eine subjektive *actual knowledge* über eine Rechtsverletzung.[1206]

Demnach hat der Host-Provider tatsächliche Kenntnis von einer Urheberrechtsverletzung i.S.d. § 512 (c) (A) (i) DMCA, sofern er subjektiv Kenntnis über urheberrechtsverletzendes Material auf seinem System verfügt. Nach der hier vertretenen Auffassung, ist allerdings zu bezweifeln, dass eine solche subjektive Kenntnis überhaupt begründet werden kann. Das Hauptproblem wird in der Praxis darin liegen, eine entsprechende subjektive Kenntnis des Host-Providers in Ermangelung der Zusendung einer *notification* zu beweisen.

(2) No awareness - Keine Red Flag knowledge

Der Host-Provider kommt zudem gem. § 512 (c) (1) (A) (ii) DMCA in den Genuss der Haftungsprivilegien, sofern er sich keiner Tatsachen oder Umstände bewusst ist, aus denen eine rechtsverletzende Handlung offensichtlich ist (*awareness*).

Die offensichtlich rechtsverletzenden Handlungen werden auch als sog. *red flags* bezeichnet, die gesetzliche Bestimmung entsprechend als *red flag*-Test.[1207]

Zu der Frage, wann genau der Host-Provider sich einer offensichtlich rechtsverletzenden Handlung bewusst ist, führen die Gesetzgebungsmaterialien folgendes aus. Der *red flag*-Test enthält

---

[1205] So auch ALS Scan, Inc. v. Remarq Commumities, Inc., 239 F.3d 619, 623 (4th Cir. 2001), *„[...] had actual knowledge of the infringing nature [...]*"; Finley-Hunt, 2013 Colum. Bus. L. Rev. 906, 943, *„[...] the statutory language, history, and subsequent interpretation support the conclusion that knowledge of the file's infringing nature is necessary, rather than just knowledge that the activity is taking place.*"; Reese, 32 Colum. J. L. & Arts 427, 433 f. (2009).

[1206] A.A. Rozsnyai, 2 Shidler J. L. Com & Tech. 15 (2006): *„[...] it will have 'knowledge or awareness' of allegedly infringing activity under § 512(c) [...]".*

[1207] H.R. Rep. 105-551(II), S. 53; S. Rep. 105-190, S. 44.

sowohl ein subjektives als auch ein objektives Element.[1208] Zur Feststellung, ob sich ein Host-Provider einer *red flag* bewusst war, muss das subjektive Bewusstsein der streitgegenständlichen Tatsachen und Umstände bestimmt werden.[1209] Für die Ermittlung, ob diese Tatsachen oder Umstände eine *red flag* darstellen, muss hingegen ein objektiver Standard angewandt werden.[1210] Die Frage ist hier, ob die rechtsverletzende Handlung für eine vernünftige Person (*reasonable person*) offensichtlich gewesen wäre.[1211]

Damit unterscheidet sich die *red flag knowledge* von der im *common law* etablierten *constructive knowledge*, dem sog. Kennenmüssen, dadurch, dass diese neben dem objektiven Element noch ein subjektives Element enthält.[1212]

Die Gerichte haben sich bei der Bestimmung der *red flags* eng an diesen Ausführungen der Gesetzgebungsmaterialien orientiert.[1213] Der Unterschied zwischen *actual* und *red flag knowledge* liege somit zwischen einem objektiven bzw. subjektiven Standard.[1214] Während *actual knowledge* danach verlange, dass der Host-Provider tatsächlich oder eben subjektiv von der spezifischen Rechtsverletzung Kenntnis habe, widme sich der *red flag*-Test der Frage, ob der Provider sich subjektiv Tatsachen bewusst war, die eine spezifische Rechtsverletzung einer vernünftigen Person objektiv offensichtlich gemacht hätte.[1215]

Allerdings haben sich die Gerichte bislang damit schwer getan, das Vorliegen einer *red flag knowledge* zu bejahen.[1216] Im Schrifttum

---

[1208] H.R. Rep. 105-551(II), S. 53; S. Rep. 105-190, S. 44.
[1209] H.R. Rep. 105-551(II), S. 53; S. Rep. 105-190, S. 44.
[1210] H.R. Rep. 105-551(II), S. 53; S. Rep. 105-190, S. 44.
[1211] H.R. Rep. 105-551(II), S. 53; S. Rep. 105-190, S. 44.
[1212] Chang, 28 Cardozo Arts & Ent. L.J. 195, 202 (2010). Insoweit irrigerweise die *red flag knowledge* mit der *constructive knowl*edge gleichsetzend: Agress, J. Bus. Entrepreneurship & L. 180, 210 (2011); McMahon, 37 L.A. Law. 28, 31 (2014).
[1213] Columbia Pictures Industries, Inc. v. Fung, 710 F.3d 1020, 1043 (9th Cir. 2013); UMG Recordings, Inc. v. Shelter Capital Partners, 718 F.3d 1006, 1026 (9th Cir. 2013); Viacom Intern., Inc. v. YouTube, Inc., 676 F.3d 19, 31 (2nd Cir. 2012).
[1214] Viacom Intern., Inc. v. YouTube, Inc., 676 F.3d 19, 31 (2nd Cir. 2012).
[1215] Viacom Intern., Inc. v. YouTube, Inc., 676 F.3d 19, 31 (2nd Cir. 2012).
[1216] Der bislang einzig bekannte Fall in dem *red flag knowledge* bejaht wurde: Columbia Pictures Industries, Inc. v. Fung, 710 F.3d 1020, 1043 f. (9th Cir. 2013)

gibt es Stimmen, die daher geltend machen, dass es nach der Rechtsprechung der Gerichte unmöglich sei, eine *red flag knowledge* zu etablieren.[1217] Die Gerichte hätten die *red flag knowledge* vielmehr mit der *actual knowledge* verschmolzen und damit die gesetzlichen Vorgaben ignoriert.[1218] Diese Interpretation der *red flag knowledge* sei daher mit der Intention des Kongresses unvereinbar.[1219]

In *Columbia v. Fung* hat der *Ninth Circuit* mittlerweile aber das Vorliegen einer *red flag knowledge* bejaht.[1220] Grund hierfür waren zahlreiche Beweise, dass der Host-Provider seine Nutzer dazu drängte, spezifische urheberrechtlich geschützte Werke hoch- und herunterzuladen und denjenigen Nutzern, die auf der Suche nach urheberrechtlich geschützten Filmen waren, insoweit auch Hilfestellung geleistet hat, u.a. dahingehend, das urheberrechtliche Material auf DVD zu brennen.[1221] Das Gericht stellte fest, dass das streitgegenständliche Material ausreichend aktuell und bekannt war, weshalb es für eine vernünftige Person objektiv offensichtlich gewesen sei, dass das Material urheberrechtlich geschützt und rechtsverletzend genutzt wurde.[1222] Da der Host-Provider keine dieser Beweislage widersprechenden Fakten im Hinblick auf die streitgegenständlichen Werke erbracht habe, sei davon auszugehen, dass eine *red flag knowledge* auch hinsichtlich dieser Werke vorlag.[1223]

Abgelehnt hat der *Ninth Circuit* allerdings beispielsweise die Konstruktion einer *red flag* aufgrund der Bezeichnung der Webseiten als „illegal.net“ oder „stolencelebritypics.com“.[1224] Diese Bezeichnungen an sich begründeten noch keine *awareness*,

[1217] Chang, 28 Cardozo Arts & Ent. L.J. 195, 203 (2010).
[1218] Chang, 28 Cardozo Arts & Ent. L.J. 195, 203 (2010).
[1219] Chang, 28 Cardozo Arts & Ent. L.J. 195, 203 (2010).
[1220] Columbia Pictures Industries, Inc. v. Fung, 710 F.3d 1020, 1043 (9th Cir. 2013).
[1221] Columbia Pictures Industries, Inc. v. Fung, 710 F.3d 1020, 1043 (9th Cir. 2013).
[1222] Columbia Pictures Industries, Inc. v. Fung, 710 F.3d 1020, 1043 (9th Cir. 2013).
[1223] Columbia Pictures Industries, Inc. v. Fung, 710 F.3d 1020, 1043 (9th Cir. 2013).
[1224] Perfect 10, Inc. v. CCBill LLC, 488 F.3d 1102, 1114 (9th Cir. 2007).

da sie nicht unbedingt den tatsächlichen Inhalt der Webseite wiedergäben, sondern vielmehr ein Versuch sein könnten, hierdurch eine größere Anziehung auf die Nutzer auszuüben.[1225] Es sei jedenfalls nicht Aufgabe des Host-Providers zu bestimmen, ob die auf solchen Seiten zugänglichen Fotografien tatsächlich rechtsverletzend sind.[1226]

Die h.M. geht zudem davon aus, dass auch die *red flags* auf eine spezifische Rechtsverletzung gerichtet sein müssen.[1227] Ein generelles Bewusstsein, dass der Dienst zur Begehung von Urheberrechtsverletzungen genutzt wird, ist nicht ausreichend.[1228] Fraglich ist allerdings, wie sich die neueste Rechtsprechung des *Ninth Circuit* in *Columbia v. Fung* hiermit vereinbaren lässt. Das Gericht hat zwar letztens Endes auch auf eine spezifische Kenntnis der streitgegenständlichen Werke abgestellt, allerdings hat es diese Kenntnis aufgrund vorliegender Beweise dahingehend, dass der Host-Provider Kenntnis von einer Großzahl einzelner Werke hatte und aufgrund fehlender gegensätzlicher Beweisführung des Host-Providers, auch im Hinblick auf die streitgegenständlichen Werke impliziert. Im Endeffekt bedeutet dies, dass der Rechteinhaber lediglich zu beweisen hat, dass der Host-Provider Kenntnis von einzelnen rechtsverletzenden Werken hat und der Host-Provider dann beweispflichtig dahingehend ist, dass er von den streitgegenständlichen Materialien eben keine Kenntnis hatte.

(a) Kritik

Starken Gegenwind haben insbesondere die Ausführungen hinsichtlich einer subjektiven und objektiven Kenntnis einer spezifischen Rechtsverletzung von *Nimmer* erfahren.[1229] Der ihm

[1225] Perfect 10, Inc. v. CCBill LLC, 488 F.3d 1102, 1114 (9th Cir. 2007).
[1226] Perfect 10, Inc. v. CCBill LLC, 488 F.3d 1102, 1114 (9th Cir. 2007).
[1227] Viacom Intern., Inc. v. YouTube, Inc., 676 F.3d 19, 31 (2nd Cir. 2012); UMG Recordings, Inc. v. Shelter Capital Partners, 667 F.3d 1022, 1038 (9th Cir. 2011); Carroll, U. Miami L. Rev. 421, 428 (2014); Rasenberger/Pepe, 59 J. Copyright Soc'y U.S.A., 627, 668 ff. (2012); Williams, 48 New Eng. L. Rev. 657, 666 (2014); Wiseman, 14 Nev. L.J. 210, 218 (2013).
[1228] Viacom Intern., Inc. v. YouTube, Inc., 676 F.3d 19, 31 (2nd Cir. 2012); UMG Recordings, Inc. v. Shelter Capital Partners, 667 F.3d 1022, 1038 (9th Cir. 2011).
[1229] Nimmer on Copyright, § 12B.04 [b].

zufolge anzusetzende Maßstab fragt danach, ob der Host-Provider absichtlich trotz offensichtlicher Urheberrechtsverletzungen (*blatant copyright infringements*), derer er sich bewusst war, wie gewohnt vorgegangen ist, ohne Abhilfe zu schaffen.[1230]

Der *Ninth Circuit* habe in *UMG v. Veoh* aus politischen Erwägungen heraus geurteilt und dabei völlig den Wortlaut der gesetzlichen Bestimmung außer Acht gelassen.[1231] Während bei der tatsächlichen Kenntnis von „actual knowledge that *the* material or *an* activity [...] is infringing" die Rede ist, verlangt der Gesetzgeber bei der *red flag*-Bestimmung lediglich, dass der Host-Provider *„is not aware of facts or circumstances from which infringing activity is apparent"*.[1232] Er hat bei der Bestimmung der *red flag knowledge* folglich den bestimmten Artikel weggelassen. Deshalb beziehe sich die tatsächliche Kenntnis auf eine spezifische Rechtsverletzung während die *red flag*-Bestimmung Allgemeinheiten (*generalities*) behandele.[1233] Das allgemeine Bewusstsein (*general awareness*) des Host-Providers, dass es auf seiner Seite zu massenhaften Urheberrechtsverletzungen komme, könne demnach bereits ausreichend sein, um eine *red flag* Kenntnis zu begründen, diese müsse sich nicht auf spezifische, konkrete Fälle von Urheberrechtsverletzungen beziehen.[1234]

Nimmer widerspricht zudem der Schlussfolgerung des *Ninth* und *Second Circuit*, dass *actual knowledge* eine subjektive Kenntnis sei während *red flag knowledge* objektiv sei. Er begründet dies damit, dass der Wortlaut des Gesetzestextes ebenso bzw. noch plausibler dahingehend interpretiert werden könne, dass *„actual knowledge that the material ... is infringing"* eine objektive Sichtweise kennzeichne während *„aware[ness] of facts that make infringement apparent"* auf eine subjektive hinweise.[1235] Auch die Gesetzgebungsmaterialien würden der Interpretation des *Ninth* und

[1230] Nimmer on Copyright, § 12B.04 [b] [i].
[1231] Nimmer on Copyright, § 12B.04 [b] [ii].
[1232] Nimmer on Copyright, § 12B.04 [b] [ii].
[1233] Nimmer on Copyright, § 12B.04 [b] [ii].
[1234] Nimmer on Copyright, § 12B.04 [b] [ii]; so auch Rasenberger/Pepe, 59 J. Copyright Soc'y U.S.A., 627, 694 (2012).
[1235] Nimmer on Copyright, § 12B.04 [b] [iii].

Second Circuit entgegenstehen.[1236] Diese würden lediglich für den Unterabsatz der *red flag*-Bestimmung eine objektive und subjektive Variable voraussetzen.[1237] Dem Unterabsatz der *actual knowled*ge nun einen subjektiven Sinngehalt zuzusprechen, würde diesen überflüssig machen, da bereits die *red flag knowledge* sowohl eine objektive als auch einen subjektive Komponente beinhalte. [1238]

Auch die Begründung des *Second Circuit* in *Viacom v. YouTube* im Hinblick auf die Verpflichtung zur Sperrung/Löschung verwirft er ohne tiefergehende Begründung als nicht schlüssig.[1239]

Das Gericht hatte hier ausgeführt, dass auch die *red flag knowledge* eine Kenntnis bezogen auf eine spezifische Rechtsverletzung voraussetze, da ansonsten die Verpflichtung zur Beseitigung dieser völlig gestaltlos sei.[1240]

Zudem spricht sich *Nimmer*, mit Bezug auf die Gesetzgebungsmaterialien, dafür aus, dass Webseiten, die sich dazu entscheiden, eine offensichtlich rechtswidrige Bezeichnung in ihrer URL zu wählen, wie bspw. „pirate", „bootleg" oder sonstige umgangssprachliche Begriffe, bereits den Schutz des *safe harbor* verlieren, ohne dass irgendeine Art von Rechtsverletzung oder ein bewusstes Wegschauen des Host-Providers nachgewiesen werden muss.[1241]

Nimmer kommt folglich zu dem Schluss, dass dem *Ninth* und *Second Circuit* in dieser Hinsicht nicht gefolgt werden sollte.[1242]

Seine Lösung stellt sich wie folgt dar: Erhält der Host-Provider generelle Kenntnis von einer Seite mit einem offenkundig überwiegenden Teil rechtsverletzender Inhalte, so hat er schlicht den Zugang zu dieser zu sperren.[1243]

Eine weniger drastische Lösung liefern *Rasenberger/Pepe*, indem sie dem Host-Provider, sofern er eine generelle Kenntnis darüber

[1236] Nimmer on Copyright, § 12B.04 [b] [iii].
[1237] Nimmer on Copyright, § 12B.04 [b] [iii].
[1238] Nimmer on Copyright, § 12B.04 [b] [iii].
[1239] Nimmer on Copyright, § 12B.04 [b] [iii].
[1240] Nimmer on Copyright, § 12B.04 [b] [iii].
[1241] Nimmer on Copyright, § 12B.04 [b| [iii].
[1242] Nimmer on Copyright, § 12B.04 [b] [iv].
[1243] Nimmer on Copyright, § 12B.04 [d].

hat, dass sein Dienst für massenhafte Urheberrechtsverletzungen genutzt wird, dazu angehalten sein sollte, entsprechende einfache Schritte zu unternehmen, um die Rechtsverletzungen herauszufiltern und zu entfernen, bspw. auch durch Einsatz von Filtertechnologien.[1244] Dem würde auch nicht § 512 (m) DMCA entgegenstehen, da dieser lediglich klarstelle, dass Überwachungs- und Nachforschungspflichten des ISP keine Voraussetzung für die Inanspruchnahme der *safe harbor* Privilegien sind.[1245] Sofern der Host-Provider allerdings Kenntnis von *red flags* habe, sei er auch dazu verpflichtet, durch einfache Maßnahmen diesen *red flags* nachzugehen um diese zu lokalisieren und anschließend entfernen zu können.[1246]

(b) Bewertung

Insbesondere der Analyse von *Nimmer* können einige gewichtige Argumente entgegen gebracht werden.

Zu bezweifeln ist zunächst, dass der Gesetzgeber damals bei der Formulierung der *actua*l und *red flag knowledge* die von *Nimmer* vorgeschlagene Interpretation vor Augen hatte. Dagegen spricht, dass auch der den beiden Bestimmungen folgende Unterabsatz, der die Verpflichtung zur Entfernung/Sperrung des Materials regelt, von einer Verpflichtung des Host-Providers zu *„expeditiously [to] remove, or disable access to, the material"* spricht. Da diese Regelung sowohl im Falle der *actual* als auch der *red flag knowledge* Anwendung findet, stellt sich die Frage, welches Material vom Host-Provider zu entfernen bzw. zu sperren ist, wenn sich die *red flag knowledge* nicht auf ein spezifisches und bestimmbares Material bezieht sondern darauf, dass es grundsätzlich zu Rechtsverletzungen auf der Seite des Host-Providers kommt.

Auch der weiteren Analyse hinsichtlich des objektiven und subjektiven Sinngehalts der beiden Bestimmungen können gewichtige Argumente entgegengebracht werden.

[1244] Rasenberger/Pepe, 59 J. Copyright Soc'y U.S.A., 627, 694 (2012).
[1245] Rasenberger/Pepe, 59 J. Copyright Soc'y U.S.A., 627, 687 (2012).
[1246] Rasenberger/Pepe, 59 J. Copyright Soc'y U.S.A., 627, 687 (2012).

Insbesondere die Interpretation der *actual knowledge* als objektives Kriterium und der *red flag knowledge* als subjektives widerspricht der folgenden im Urheberrecht geltenden Maxime. Danach wird als *actual knowledge* eine subjektive Kenntnis bezeichnet, eine direkte und eindeutige Kenntnis (*direct and clear knowledge*), während *constructive knowledge* eine objektive Kenntnis darstellt und zwar *„knowledge that one using reasonable care or diligence should have, and therefore that is attributed by law to a given person“*.[1247] Dies widerspricht der Auffassung Nimmers, dass die *actual knowledge* i.S.d. § 512 DMCA eine objektive Kenntnis sei.

Zudem wird der Unterabsatz der *actual knowledge* nicht bereits dadurch obsolet, dass die *red flag knowledge* sowohl ein subjektives als auch ein objektives Kriterium enthält. Denn bevor das subjektive Merkmal der Kenntnis über eine spezifische *red flag* überhaupt zum Einsatz kommt, muss zunächst objektiv etabliert werden, dass es sich um eine *red flag* handelt.[1248] In der Praxis bedeutet dies, dass der Host-Provider subjektiv Kenntnis hinsichtlich eines spezifischen Materials auf seiner Seite haben muss und dass die Rechtswidrigkeit dieses Materials objektiv für eine vernünftige Person offensichtlich ist. Im Gegensatz hierzu enthält die *actual knowledge* lediglich ein subjektives Merkmal, weshalb hier die tatsächliche Kenntnis über eine spezifische Rechtsverletzung vorausgesetzt wird.

Auch *Nimmers* Ausführungen hinsichtlich der Sperrungsverpflichtung im Falle einer *general knowledge* überzeugen nicht. So geht er mit keinem Wort auf die Gefahren einer solchen Interpretation, nämlich die Sperrung von legalen Inhalten, ein. Fraglich ist auch, wann genau eine Seite aus hauptsächlich rechtswidrigen Inhalten besteht. Wie hoch muss der Anteil der rechtswidrigen Inhalte sein, um die Sperrung legaler Inhalte in Kauf zu nehmen und wie kann der Host-Provider überhaupt eine entsprechende Evaluation vornehmen? All diese

[1247] Black's law dictionary, S. 1004; Högberg, 106 Colum. L. Rev. 909, 920 (2006).
[1248] Entertainment Law & Litigation, § 4.08 [2] [d].

offenen Fragen lassen erhebliche Zweifel an einer entsprechenden Auslegung der *red flag* Bestimmung aufkommen.

Sofern sich *Nimmer* auf die Gesetzgebungsmaterialien bezieht, welche ausführen, dass Piraterie-Webseiten (*pirate sites*) eine *red flag* darstellen, wenn sie Musikstücke, Software, Filme und Bücher zum unautorisierten Download bereithalten und deren illegale Natur bereits durch einen flüchtigen Blick offenbart wird, können auch dieser Begründung überzeugende Argumente entgegengebracht werden.[1249] Zunächst behandelt der zitierte Absatz innerhalb der Gesetzgebungsmaterialien nicht den Host-Provider, sondern die *Information Location Tools*, welche in § 512 (d) DMCA geregelt sind. Auch wenn der Wortlaut hinsichtlich der *actual* und *red flag knowledge* identisch zu § 512 (c) DMCA ist, so bezieht sich der von *Nimmer* genannte Ausschnitt lediglich auf *Information Location Tools*, deren Mitarbeiter, beispielsweise der *editor* oder *reviewer,* zuvor die streitgegenständliche verlinkte Webseite aufgerufen haben und bei denen diese bereits zu diesem Zeitpunkt eine eindeutige *pirate site* gewesen ist.[1250] Es ging dem Gesetzgeber also lediglich darum, das Verlinken von Seiten, die von vornherein offensichtlich rechtswidriger Natur sind, zu verhindern. Dadurch sollten diejenigen Provider von dem Schutz der Vorschrift ausgenommen werden, die zuvor durch ihre Mitarbeiter die offenkundige *pirate site* aufgerufen haben und diese in der Folge trotz alledem in ihrem Verzeichnis gelistet haben.

(c) Ergebnis

Aufgrund der zuvor genannten Überlegungen ist es angebracht, dem *Ninth* und *Second Circuit* zu folgen und für das Bejahen einer *red flag* das Vorliegen einer spezifischen und nicht lediglich generellen Kenntnis vorauszusetzen. Dabei müssen *red flags* so

[1249] Siehe hierzu H.R. Rep. 105-551(II), S. 57 f.; S. Rep. 105-190, S. 49.

[1250] H.R. Rep. 105-551(II), S. 57f.; S. Rep. 105-190, S. 49: *„[...] if the copyright holder could prove that the location was clearly, at the time the directory provider viewed it, a 'pirate' site [...]."*

offensichtlich sein, dass es keiner weiteren Nachforschung seitens des Host-Providers bedarf.[1251]

Sofern ein Teil des Schrifttums zu bedenken gibt, dass es schwierig sei, sich ein Szenario vorzustellen, in welcher eine *red flag knowledge*, aber keine *actual knowledge* vorliege[1252], kann dem nicht gefolgt werden. Auch der *Second Circuit* führt explizit aus, dass die *red flag*-Bestimmung und die *actual knowledge* Bestimmung jeweils unabhängige Arbeit leisteten.[1253]

Red flag knowledge wird immer dann vorliegen, wenn der Host-Provider subjektiv Kenntnis von einem bestimmten Inhalt hatte, dessen Rechtswidrigkeit für eine vernünftige Person offensichtlich gewesen wäre.

In dem bislang einzigen Fall, der eine *red flag knowledge* bejahte, hat der *Ninth Circuit* dem Host-Provider jedoch eine Beweispflicht dahingehend auferlegt, dass, sofern es Beweise dafür gibt, dass der Host-Provider Kenntnis von rechtsverletzenden Werken innerhalb seines Dienstes hatte, er keine entsprechende Kenntnis hinsichtlich der streitgegenständlichen Werke hatte.[1254]

Derzeit ist ein Fall vor dem *Second Circuit* anhängig, bei dem es um die Frage geht, ob dadurch, dass die Mitarbeiter eines Host-Providers sich die streitgegenständlichen Videos angesehen haben und diese erkennbar urheberrechtlich geschützte Musik enthielten, eine *red flag knowledge* begründet werden könne.[1255] Der Host-Provider machte hier geltend, dass für die Mitarbeiter nicht offensichtlich gewesen sei, ob die Videos Urheberrechte verletzten, da es sich um Fälle des *fair use* handeln könne.[1256]

[1251] Perfect 10, Inc. v. CCBill LLC, 488 F.3d 1102, 1114 (9th Cir. 2007); Capitol Records, Inc. v. MP3Tunes, LLC, 821 F.Supp.2d 627, 644 (S.D.N.Y. 2011); Finlay-Hunt, Colum. Bus. L. Rev. 906, 947 (2013).

[1252] Chang, 28 Cardozo Arts & Ent. L.J. 195, 204 (2010); Rasenberger/Pepe, 59 J. Copyright Soc'y U.S.A., 627, 680 (2012).

[1253] Viacom Intern., Inc. v. YouTube, Inc., 676 F.3d 19, 31 (2nd Cir. 2012).

[1254] Columbia Pictures Industries, Inc. v. Fung, 710 F.3d 1020, 1043 (9th Cir. 2013).

[1255] Capitol Records, LLC v. Vimeo, LLC, 972 F.Supp.2d 537, 556.

[1256] Capitol Records, LLC v. Vimeo, LLC, 972 F.Supp.2d 537, 545, bei den meisten der Videos handelte es sich um sog. „*lip-dubs*", welche einzelne Personen zeigen, die ihren Mund bewegen während urheberrechtlich geschützte Musik gespielt wird.

Es bleibt abzuwarten, wie der *Second Circuit* den vorliegenden Fall bewertet und somit auch das gesetzliche Konstrukt der *red knowledge* mit Leben füllt.

Wie jedoch zuvor ausgeführt, liegt nach der hier vertretenen Ansicht eine *red flag knowledge* immer dann vor, wenn der Host-Provider positiv Kenntnis hinsichtlich eines spezifischen Materials hat und die Rechtswidrigkeit dieses Materials objektiv für eine vernünftige Person offensichtlich ist. Ist folglich nicht auszuschließen, dass es sich um einen Fall von *fair use* handelt, kann dem Host-Provider auch keine *red flag knowledge* angelastet werden.

Nicht ausreichend für das Vorliegen einer *red flag* ist jedenfalls eine fehlerhafte *notification* i.S.d. § 512 (c) (3) (B) (i) DMCA[1257]

(3) Sonderfall: Willful Blindness

Das Prinzip des absichtlichen Augenverschließens (*willfull blindness*) hat seinen Ursprung im *case law* des Strafrechts.[1258] Danach liegt Kenntnis vor, wenn der Beklagte subjektiv von der hohen Wahrscheinlichkeit einer bestimmten Straftat wusste und vorsätzlich Maßnahmen ergriff um eine objektive Kenntnis der genauen Umstände zu verhindern.[1259]

Für den Bereich des Patentrechts hat der *Supreme Court* die Voraussetzungen wie folgt festgesetzt:

„First, the defendant must subjectively believe that there is a high probability that a fact exists. Second, the defendant must take deliberate actions to avoid learning of that fact.“[1260] Der Beschuldigte muss folglich zunächst subjektiv an die hohe Wahrscheinlichkeit einer Rechtsverletzung glauben und anschließend bewusste Handlungen vornehmen, um zu verhindern, dass er tatsächliche Kenntnis hiervon erlangt.

[1257] Siehe hierzu ausführlich S. 309.
[1258] Finlay-Hunt, Colum. Bus. L. Rev. 906, 920 (2013); Case Comment, 126 Harv. L. Rev. 645, 645 (2012).
[1259] Finlay-Hunt, Colum. Bus. L. Rev. 906, 920 (2013).
[1260] Global-Tech Appliancs, Inc. v. SEB S.A., 131 S.Ct. 2060, 2063 (2011).

Eingang ins Urheberrecht fand diese Lehre durch den *Seventh Circuit* in *In re Aimster Copyright Litigation*[1261]. Dort hat das Gericht ausgeführt, das *willful blindness* im Urheberrecht einer Kenntnis gleichsteht.[1262]

Fraglich ist allerdings, wie sich diese Lehre in die Kenntnis im Rahmen des DMCA einfügt.

(a) Actual knowledge/Awareness durch Willful Blindness

In *Viacom v. YouTube* hat der *Second Circuit* sich ausführlich mit der Frage der Vereinbarkeit der *willful blindness*-Doktrin mit den Bestimmungen des DMCA beschäftigt. Er führte zunächst aus, dass eine gesetzliche Bestimmung einen *common law* Grundsatz lediglich aufhebt, sofern das Gesetz direkt die durch das *common law* geregelte Frage adressiert.[1263]

Bei der Beantwortung der Frage, ob eine solche Adressierung vorliegt, kam das Gericht zu dem Schluss, dass die Bestimmung, welche am ehesten die *willful blindness*-Doktrin beeinflusse, § 512 (m) DMCA sei.[1264] Dieser besagt, dass der DMCA *safe harbor* nicht davon abhängig gemacht werden darf, dass dem ISP eine Verpflichtung zur Überwachung seines Dienstes auferlegt wird. Diese Bestimmung stehe damit im Widerspruch zu einer umfassenden *common law* Verpflichtung, bei einer *general awareness* von Rechtsverletzungen seine Dienste zu überwachen, um diese Rechtsverletzungen aufzuspüren.[1265]

Da *willful blindness* allerdings nicht als aktive Verpflichtung zur Überwachung der Dienste des ISP verstanden werden könne, kommt der *Second Circuit* schließlich zu dem Schluss, dass § 512 (m) DMCA die *willful blindness*-Doktrin zwar einschränke, aber nicht komplett aufhebe.[1266]

[1261] In re Aimster Copyright Litigation, 334 F.3d 643 (2003).
[1262] In re Aimster Copyright Litigation, 334 F.3d 643, 650 (2003).
[1263] Viacom Intern., Inc. v. YouTube, Inc., 676 F.3d 19, 35 (2nd Cir. 2012).
[1264] Viacom Intern., Inc. v. YouTube, Inc., 676 F.3d 19, 35 (2nd Cir. 2012).
[1265] Viacom Intern., Inc. v. YouTube, Inc., 676 F.3d 19, 35 (2nd Cir. 2012).
[1266] Viacom Intern., Inc. v. YouTube, Inc., 676 F.3d 19, 35 (2nd Cir. 2012).

Im Ergebnis könne deshalb die *willful blindness*-Doktrin im Einzelfall zur Anwendung kommen, um *knowledge* oder *awareness* nachzuweisen.[1267]

(b) Kritik

Teilweise wird die Meinung vertreten, dass die *willful blindness*-Doktrin bereits durch die *red flag*-Bestimmung erfasst wurde.[1268] Gestützt wird diese Ansicht hauptsächlich auf die Gesetzgebungshistorie. Dort wird im Rahmen der Voraussetzungen zur Privilegierung der *Information Location Tools* sowohl für diese als auch für den Host-Provider ausgeführt, dass sie keine Pflicht trifft, Urheberrechtsverletzungen aufzuspüren, sie sich allerdings nicht für den *safe harbor* qualifizieren, sofern sie red flags wissentlich ignorieren (*„[...] turned a blind eye to „red flags" of obvious infringement"*).[1269] Sowohl *red flag knowledge* als auch *willful blindness* stellen zunächst die Frage, ob der Beklagte subjektiv Kenntnis von einem Inhalt hatte und gehen dann zu einer objektiven Analyse über.[1270] Diese objektive Analyse fragt im Falle der *red flag knowledge*, ob die Rechtsverletzung für eine vernünftige Person objektiv offensichtlich gewesen wäre, im Falle der *willful blindness*, ob der Beklagte absichtlich Maßnahmen ergriffen hat, um zu verhindern, von der Rechtsverletzung Kenntnis zu erlangen.

Red flag knowledge befriedige demnach den Zweck, Fälle von *willful blindness* zu verhindern.[1271] Da die *willful blindness* zudem auf eine spezifische Rechtsverletzung bezogen sein müsse, falle es schwer, sich einen Fall vorzustellen, in dem der Beklagte weder objektive noch subjektive Kenntnis im Sinne der *red flag* Bestimmung habe, dafür aber *willfully blind* handele.[1272]

[1267] Viacom Intern., Inc. v. YouTube, Inc., 676 F.3d 19, 35 (2nd Cir. 2012).
[1268] Columbia Pictures Industries, Inc. v. Fung, No. CV 06-5578 SVW(JCx), 2009 WL 6355911 (C.D. Cal. Dec. 21, 2009) at *16; Finlay-Hunt, Colum. Bus. L. Rev. 906, 906 (2013); Ludwig, Boston College Intellectual Property & Technology Forum, 4 (2006).
[1269] H.R. Rep. 105-551(II), S. 57; S. Rep. 105-190, S. 48.
[1270] Finlay-Hunt, Colum. Bus. L. Rev. 906, 946 (2013).
[1271] Finlay-Hunt, Colum. Bus. L. Rev. 906, 958 (2013).
[1272] Finlay-Hunt, Colum. Bus. L. Rev. 906, 958 (2013).

Fraglich sei zudem, wie der Host-Provider absichtlich Maßnahmen ergreifen könne, um zu verhindern, von der Rechtsverletzung Kenntnis zu erlangen, ohne dabei § 512 (m) DMCA zuwiderzuhandeln.[1273]

Einer anderen Meinung nach sollte die Prüfung der *willful blindness* um eine Motiv-Analyse ergänzt werden.[1274] Diese würde voraussetzen, dass der Beklagte speziell durch den Wunsch motiviert wurde, einer Haftung zu entgehen.[1275] Diese Analyse würde somit sicherstellen, dass diejenigen Host-Provider, die legitime Gründe dafür haben, dass sie es verpasst haben, einem speziellen dringenden Verdacht nachzugehen, von denjenigen, die dadurch bewusst das Gesetz umgehen wollen, abgegrenzt werden.[1276]

(c) Bewertung

Der Gesetzgebungshistorie ist zu entnehmen, dass die Bestimmungen des DMCA die allgemeinen Haftungsmaßstäbe unberührt lassen sollen und lediglich eine Serie von *safe harbor* im Falle einer festgestellten Verantwortlichkeit nach dem Urheberrechtsgesetz oder *common law* begründen.[1277] Das bedeutet im Umkehrschluss, dass die Kenntnis im Sinne von § 512 (c) (1) (A) (i) und (ii) DMCA unabhängig von den einschlägigen Verantwortlichkeiten nach *commmon law* ist und somit zu deren Bestimmung auch andere Maßstäbe angelegt werden müssen.

Verfehlt sind daher zunächst die Ausführungen des *Second Circuit* hinsichtlich der Aufhebung bzw. Einschränkung des *common law* Prinzips der *willful blindness*. Zwar gibt es generell den Grundsatz,

---

[1273] Finlay-Hunt, Colum. Bus. L. Rev. 906, 958 (2013).
[1274] U.S. v. Heredia, 483 F.3d 913, 929 (2007) (Kleinfeld, J., concurring); Case Comment, 126 Harv. L. Rev. 645, 645 (2012); Case Comment, 121 Harv. L. Rev., 1245, 1252 (2008).
[1275] Case Comment, 126 Harv. L. Rev. 645, 651 (2012).
[1276] Case Comment, 126 Harv. L. Rev. 645, 651 (2012).
[1277] H.R. Rep. 105-551(II), S. 50: *„[...] new Section 512 is not intended to imply that a service provider is or is not liable as an infringer either for conduct that qualifies for a limitation of liability or for conduct that fails to so qualify.*“; S. Rep. 105-190, S. 19: *„Rather than embarking upon a wholesale clarification of these doctrines, the Committee decided to leave its current law in its evolving state and, instead, to create a series of 'safe harbors' for certain common activities of service providers.“*

dass ein *common law* Prinzip lediglich dann aufgehoben wird, wenn die gesetzliche Bestimmung die durch das *common law* geregelte Frage gezielt anspricht.[1278] Allerdings weisen die Gesetzgebungsmaterialien ja explizit darauf hin, dass diese allgemeinen Haftungsmaßstäbe gerade unberührt bleiben sollen.

Geht man also der Frage nach, wann eine *red flag* im Sinne des DMCA vorliegt, so ist dies unabhängig von den geltenden *common law* Prinzipien der mittelbaren Haftung zu bestimmen.

Korrekt ist daher die Ansicht, dass der Gesetzgeber bei Schaffung der *safe harbor* bereits Fälle von *willful blindness* im Hinterkopf hatte und diesen durch die entsprechende Formulierung der *red flag* Bestimmung abdecken wollte. Diese Ansicht wird auch eindeutig durch die Gesetzgebungsmaterialien gestützt.[1279]

Im Ergebnis ist daher dem *Second Circuit* zuzustimmen. Sofern der Host-Provider absichtlich die Augen vor spezifischen Rechtsverletzungen im Sinne einer *willful blindness* verschließt, wird eine *awareness* hinsichtlich der spezifischen Urheberrechtsverletzung im Sinne des § 512 (c) (1) (A) (ii) DMCA vermutet. Sofern er bezüglich der spezifischen Rechtsverletzung keine Abhilfe schafft, ist er schließlich nach den allgemeinen Grundsätzen verantwortlich.

(4) Keine zügige Entfernung bzw. Sperrung des Materials

Gem. § 512 (c) (1) (A) (iii) DMCA hat der Host-Provider, nachdem er *actual knowledge* oder *awareness* erlangt hat, zügig (*expeditiously*) das Material zu entfernen bzw. den Zugang hierzu zu sperren.

Diese Bestimmung deckt sich teilweise mit § 512 (c) (1) (C) DMCA, der eine entsprechende Pflicht zur Entfernung des Materials bzw. Sperrung des Zugangs nach Erhalt einer *notification* regelt.

Hierdurch soll zum einen sichergestellt werden, dass den Host-Provider bereits sobald er Kenntnis bzw. das Bewusstsein einer

[1278] Siehe bspw. Matar v. Dichter, 563 F.3d 9,14 (2d Cir.2009).
[1279] H.R. Rep. 105-551(II), S. 57; S. Rep. 105-190, S. 48.

Rechtsverletzung hat, eine Pflicht zur Entfernung bzw. Sperrung trifft und nicht erst nach dem Erhalt einer *notification*.[1280] Zum anderen wird hierdurch auch der ISP geschützt, indem er nicht direkt seine Haftungsprivilegierung aufgrund von Kenntnis bzw. Bewusstsein einer Rechtsverletzung verliert, sondern diese durch die prompte Entfernung bzw. Sperrung weiter aufrecht erhält.

Fraglich ist, wann genau der Host-Provider *expeditiously* handelt. Es handelt sich um einen unbestimmten Rechtsbegriff, der abhängig von den spezifischen Umständen und technischen Parametern des Einzelfalls bestimmt werden muss.[1281]

Die Rechtsprechung zu diesem Punkt ist bislang eher dürftig und erging hauptsächlich im Hinblick auf § 512 (c) (1) (C) DMCA, welcher auch die prompte Entfernung des Materials bzw. Sperrung des Zugangs zu diesem vorsieht, allerdings nach Erhalt einer *notification*. Aufgrund des identischen Wortlauts, kann hier allerdings auf diese Rechtsprechung zurückgegriffen werden.[1282] Demnach bedarf es bei der Bewertung des Begriffs einer Einzelfallanalyse, die die faktischen Umstände und technischen Parameter in die Evaluierung mit einbezieht. In der Regel dürfte jedoch eine Reaktion innerhalb weniger Tage als ausreichend erachtet werden.

dd) Kein finanzieller Vorteil und keine Kontrolle

Die weitere Voraussetzung für eine Haftungsprivilegierung im Rahmen des DMCA besteht aus zwei Elementen und ist in § 512 (c) (1) (B) DMCA geregelt. Danach darf der Host-Provider keinen finanziellen Vorteil aus der rechtsverletzenden Tätigkeit ziehen, sofern er das Recht und die Möglichkeit hat, eine solche Aktivität zu kontrollieren (*financial benefit and ability to control*).

[1280] White, 24 St. John's J. Legal Comment. 811, 826 (2010).

[1281] H.R. Rep. 105-551(II), S. 53 f.; S. Rep. 105-190, S. 44; lt. Wörterbuch bedeutet *expeditious* „*acting or done in a quick and efficient way*", siehe http://www.merriam-webster.com/dictionary/expeditious, zuletzt besucht am 24.04.2016.

[1282] White, 24 St. John's J. Legal Comment. 811, 827 Fn. 101 (2010); zur genauen Bestimmung des Begriffs wird daher auf D.III.5.b)ee) verwiesen.

Die beiden Elemente erinnern stark an die beiden Voraussetzungen für das Vorliegen einer *vicarious infringement*. Es ist allerdings fraglich, ob der Gesetzgeber hiermit tatsächlich die beiden Merkmale der *vicarious liability* gesetzlich verankern wollte.

(1) Direkter finanzieller Vorteil

Der Host-Provider darf keinen finanziellen Vorteil (*direct financial benefit*) aus der rechtsverletzenden Tätigkeit ziehen.

Die Gesetzgebungsmaterialien führen hierzu aus, dass zur Bestimmung dieses Merkmals ein *common-sense, fact-based approach*, d.h. ein auf Fakten und gesundem Menschenverstand beruhender Ansatz, und kein *formalistic one*, d.h. kein formalistischer, herangezogen werden soll.[1283]

Keinen finanziellen Vorteil aus der rechtsverletzenden Tätigkeit würde beispielsweise derjenige Host-Provider ziehen, welcher ein legitimes Geschäftsmodell betreibt, bei dem alle Nutzer, seien es Rechtsverletzer oder keine Rechtsverletzer, die gleiche Art von Zahlung leisten.[1284] Deshalb würden eine einmalige Einrichtungsgebühr oder periodische Zahlungen nicht unter dieses Merkmal fallen.[1285] Auch Zahlungen, welche von der Größe der Nachricht oder der Verbindungsdauer abhängen, würden hiervon nicht erfasst.[1286]

Ein finanzieller Vorteil im Sinne des § 512 (c) (1) (B) DMCA würde jedoch dann vorliegen, wenn der Wert des vom Host-Provider zur Verfügung gestellten Services gerade in der Zugangsverschaffung zu rechtsverletzenden Materialien liegt.[1287]

Auf den ersten Blick scheint das Merkmal des finanziellen Vorteils des DMCA demnach identisch mit dem der *vicarious liability* zu sein. Dies sieht so auch der *Ninth Circuit*, indem er in *Perfect 10 v. CCBill* ausführt, dass *direct financial benefit* entsprechend dem ähnlich formulierten *common law*-Standard für *vicarious copyright*

[1283] H.R. Rep. 105-551(II), S. 54; S. Rep. 105-190, S. 44.
[1284] H.R. Rep. 105-551(II), S. 54; S. Rep. 105-190, S. 44.
[1285] H.R. Rep. 105-551(II), S. 54; S. Rep. 105-190, S. 44.
[1286] H.R. Rep. 105-551(II), S. 54; S. Rep. 105-190, S. 45.
[1287] H.R. Rep. 105-551(II), S. 54; S. Rep. 105-190, S. 45.

liability ausgelegt werden soll.[1288] In diesem Fall verneinte der *Ninth Circuit* jedoch einen solchen direkten finanziellen Vorteil, da die rechtsverletzende Tätigkeit keine hierfür notwendige Anziehungskraft (*a draw*) auf die Nutzer ausübte.[1289] Anders beurteilte der *Ninth Circuit* jedoch den Fall *Columbia v. Fung*.[1290] Das Gericht sah hier einen finanziellen Vorteil des Host-Providers, welcher direkt den rechtsverletzenden Handlungen seiner Nutzer zugerechnet werden konnte.[1291] Der Host-Provider generierte seine Einkünfte aus dem Verkauf von Werbeplatz auf seiner Webseite. Bei der Bewerbung seiner Werbeplätze wies er potentielle Inserenten auf die urheberrechtswidrigen Inhalte auf seiner Webseite hin.[1292] Zudem waren seine Einkünfte abhängig von der Anzahl der Besucher auf seiner Seite und er zog hauptsächlich solche Nutzer an, die sich an urheberrechtswidrigen Handlungen beteiligten und ermutigte diese auch zu solchen rechtswidrigen Handlungen.[1293]

(2) Bewertung

Wie insbesondere *Lee*[1294] ausführt, gibt es gewichtige Gründe, die dagegen sprechen, das Erfordernis des finanziellen Vorteils i.S.d. § 512 (c) (1) (B) DMCA dem des *common law*-Standards für *vicarious liability* gleichzusetzen.

Der *House* und *Senate Report* sprechen explizit davon, dass die Haftungsprivilegien des DMCA den ISP von einer Verantwortlichkeit in Fällen der *„direct, vicarious and contributory infringement“* schützen.[1295] Es widerspreche jeder

[1288] Perfect 10, Inc. v. CCBill LLC, 488 F.3d 1102, 1117 (9th Cir. 2007); so auch Ginsburg, 50 Ariz. L. Rev. 577, 598 (2008).
[1289] Perfect 10, Inc. v. CCBill LLC, 488 F.3d 1102, 1117 (9th Cir. 2007), *„[...] the relevant inquiry is whether the infringing activity constitutes a draw for subscribers, not just an added benefit“*.
[1290] Columbia Pictures Industries, Inc. v. Fung, 710 F.3d 1020 (9th Cir. 2013).
[1291] Columbia Pictures Industries, Inc. v. Fung, 710 F.3d 1020, 1045 (9th Cir. 2013).
[1292] Columbia Pictures Industries, Inc. v. Fung, 710 F.3d 1020, 1045 (9th Cir. 2013).
[1293] Columbia Pictures Industries, Inc. v. Fung, 710 F.3d 1020, 1045 (9th Cir. 2013).
[1294] Lee, 32 Colum. J.L. & Arts 233 (2009).
[1295] H.R. Rep. 105-551(II), S. 50; S. Rep. 105-190, S. 20.

Logik, wenn, entgegen dem Wortlaut der Gesetzgebungsmaterialien, Fälle von *vicarious infringement* von dem DMCA *safe harbor* ausgeschlossen wären, während die Haftungsprivilegien weiterhin in Fällen der *contributory infringement* Anwendung fänden.[1296]

Hätte der Kongress die *vicarious liability* von den Haftungsprivilegien ausschließen wollen, hätte er hierfür einen direkten Weg wählen können und dies im DMCA explizit im Rahmen einer Öffnungsklausel erwähnen können.[1297]

Zudem ist auch der Wortlaut der gesetzlichen Bestimmung nicht identisch mit dem der *common law vicarious liability*.[1298]

Während im DMCA die Rede davon ist, dass der Host-Provider „*does not receive a financial benefit directly attributable to the infringing activity*", haben die Gerichte den Begriff des finanziellen Vorteils im Rahmen der *vicarious liability* definiert als „*a direct financial interest in such activities*"[1299], „*a direct financial benefit*"[1300] bzw. „*an obvious and direct financial interest*"[1301].[1302]

Alleine aus dem Wortlaut wird deutlich, dass der finanzielle Aspekt im Rahmen der *vicarious liability* von den Gerichten weiter gefasst wird als im DMCA. Während nach dem *common law*-Standard bereits ein finanzielles Interesse ausreicht, verlangen die gesetzlichen Bestimmungen des DMCA einen tatsächlichen finanziellen Vorteil.[1303]

Weiterhin lässt die Wortwahl „*directly attributable to the infringing activity*" einen engeren kausalen Zusammenhang

---

[1296] Lee, 32 Colum. J.L. & Arts 233, 244 (2009).
[1297] Lee, 32 Colum. J.L. & Arts 233, 242 (2009); so bspw. in 17 U.S.C. § 1201 (c) (2): *„Nothing in this section shall enlarge or diminish vicarious or contributory liability for copyright infringement in connection with any technology, product, service, device, component, or part thereof."*
[1298] Lee, 32 Colum. J.L. & Arts 233, 240 (2009).
[1299] So z.B. Gershwin Pub. Corp. v. Columbia Artists Management, Inc., 443 F.2d 1159, 1162 (1971).
[1300] So z.B. Fonovisa, Inc. v. Cherry Auction, Inc., 76 F.3d 259, 262 (1996).
[1301] So z.B. Shapiro, Bernstein & Co. v. H. L. Green Co., 316 F.2d 304, 307 (1963).
[1302] Lee, 32 Colum., J.L. & Arts 233, 241 (2009).
[1303] Lee, 32 Colum., J.L. & Arts 233, 241 (2009).

zwischen finanziellem Vorteil und rechtsverletzender Tätigkeit vermuten.[1304]

Aufgrund dieses unterschiedlichen Wortlauts ist auch die Begründung des *Ninth Circuit*[1305] hinsichtlich der etablierten *common law* Bedeutung des *financial benefit* nicht schlüssig. Dieser führt aus, dass in Fällen, in denen der Kongress einen Begriff nutzt, der bereits eine feststehende Bedeutung unter *common law* hat, das Gericht darauf schließen muss, dass der Kongress genau diese etablierte Bedeutung in den Gesetzestext einbetten wollte, sofern das Gesetz nichts Gegenteiliges bestimmt.[1306]

Für den Terminus „*financial benefit directly attributable to the infringing activity*" existiert aber gerade keine feststehende Bedeutung im *common law*.

Zu guter Letzt würde diese Interpretation zu einer Beweislastumkehr im Rahmen der *vicarious liability* zu Lasten des Host-Providers führen. Auch wenn eine derartige Beweislastumkehr grundsätzlich im Ermessen des Kongresses steht, so ist es eher unwahrscheinlich, dass er diese durch eine derart indirekte und verschachtelte Wortwahl einführt.[1307]

Da das Merkmal des direkten finanziellen Vorteils des DMCA damit nicht dem des *common law*-Standards der *vicarious liability* entspricht, können als Ergebnis Fälle der *vicarious liability* unter die Privilegierung des DMCA fallen, sofern ein enger kausaler Zusammenhang fehlt.[1308] Denn da der finanzielle Vorteil zum Tatbestand der *vicarious liability* gehört, aber gleichzeitig das Fehlen eines solchen finanziellen Vorteils bei gleichzeitig

---

[1304] Lee, 32 Colum., J.L. & Arts 233, 241 (2009).
[1305] In Perfect 10, Inc. v. CCBill LLC, 488 F.3d 1102, 1117 (9th Cir. 2007).
[1306] Perfect 10, Inc. v. CCBill LLC, 488 F.3d 1102, 1117 (9th Cir. 2007).
[1307] Lee, 32 Colum., J.L. & Arts 233, 245 (2009).
[1308] Lee, 32 Colum., J.L. & Arts 233, 245 (2009); sog. *„partial immunity" interpretation*: a.A. Rasenberger/Pepe, 59 J. Copyright Soc'y U.S.A. 627, 692 (2012), die davon ausgehen, dass lediglich die *contributory liability* unter die Haftungsprivilegien fallen, nicht aber die *vicarious liability* (*„Congress used the vicarious liability standard wholesale in Section 512(c)(1)(B); as such, it must be assumed that it meant the vicarious liability standard--so that if a service provider is vicariously liable, it is indeed disqualified under Section 512(c)(1)(B).*").

fehlender Kontrollmöglichkeit Privilegierungsvoraussetzung ist, wären bei identischer Interpretation dieses Begriffes, Fälle von *vicarious liability* automatisch von den Privilegien ausgeschlossen.

(3) Kein Recht und keine Möglichkeit zur Kontrolle

Der Host-Provider ist ferner, auch für den Fall, dass er einen direkten finanziellen Vorteil aus der rechtsverletzenden Handlung zieht, von der Privilegierung ausgeschlossen, wenn er das Recht und die Möglichkeit hatte, eine solche Handlung zu kontrollieren (*right and ability to control*). Die Gesetzgebungsmaterialien enthalten keine Ausführungen dazu, wann eine solche Kontrolle vorliegt.

Der Wortlaut dieses Merkmals der Voraussetzung für die Privilegierung ähnelt abermals der Tatbestandsvoraussetzung der *vicarious liability*, namentlich dem Recht und der Möglichkeit der Überwachung bzw. Kontrolle der rechtsverletzenden Aktivitäten. Die Gerichte haben dieses Merkmal im Rahmen des DMCA allerdings restriktiver ausgelegt als nach dem *common law*-Standard der *vicarious liability*.

Demnach genügt jedenfalls nicht die Möglichkeit des Host-Providers, rechtswidriges Material zu entfernen, da dies ja gerade durch die *Notice and Takedown*-Bestimmung des § 512 (c) (1) (C) DMCA vorausgesetzt wird.[1309] Der Host-Provider würde also durch eine Handlung, die ihm durch den DMCA auferlegt wird, seine Privilegierung nach dem DMCA verlieren.[1310]

Verlangt wird daher etwas mehr (*something more*), als nur die Möglichkeit des Host-Providers Inhalte auf seiner Webseite oder in seinem System zu entfernen oder den Zugang zu ihnen zu sperren.[1311] Die Frage, was genau dieses *something more* ist, wurde bislang noch nicht hinreichend bestimmt.

[1309] UMG Recordings, Inc. v. Shelter Capital Partners, 718 F3d 1006, 1027 (9th Cir. 2013); IO Group, Inc. v. Veoh Networks, Inc., 586 F. Supp.2d 1132, 1151 (N.D.Cal 2008); Tur v. YouTube, Inc., No. CV064436 FMC AJWX, 2007 WL 1893635, at *3; Hendrickson v. Ebay, Inc., 165 F. Supp. 2d 1082, 1093 (C.D. Cal. 2001).

[1310] Hendrickson v. Ebay, Inc., 165 F. Supp. 2d 1082, 1093 (C.D. Cal. 2001).

[1311] Tur v. YouTube, Inc., No. CV064436 FMC AJWX, 2007 WL 1893635, at *3.

Der *C.D. California* führte diesbezüglich zunächst lediglich allgemein gehalten aus, dass dieses Merkmal eine vorangehende Möglichkeit zur Begrenzung oder Filterung von urheberrechtlich geschützten Inhalten voraussetze.[1312] Es reiche jedoch grundsätzlich nicht aus, wenn der Host-Provider freiwillig seine Dienste in gewissem Umfang überwache, um so offensichtliche Rechtsverletzungen herauszufiltern.[1313] Denn es sei nicht Sinn und Zweck dieser Bestimmung, Host-Provider, die freiwillig Bemühungen zur Bekämpfung von Piraterie ergreifen, hierfür zu bestrafen.[1314]

In *Perfect 10 v. Cybernet Ventures* bejahte das Gericht schließlich eine solche Kontrolle, da der Host-Provider u.a. die Seiten, die er hostete, vorab überprüfte und die einzelnen Webseiten-Betreibern umfassend beriet.[1315] Genau dies begründe das grundsätzlich schwer zu definierende *something more*.[1316]

Der *N.D. California* wiederum unterschied zwischen der Möglichkeit, des Host-Providers, sein System zu kontrollieren sowie der Möglichkeit die rechtswidrigen Aktivitäten auf seinem System zu kontrollieren.[1317] Nach der Auffassung des Gerichts sei die Kontrolle des Host-Providers über den Index auf seinem System nicht zu vergleichen mit der Möglichkeit, rechtsverletzende Videos zu identifizieren und zu löschen.[1318] Der Host-Provider habe im vorliegenden Fall keine Kontrolle darüber, welches Material seine Nutzer hochladen.[1319] Eine umfassende Überprüfung aller Materialien sei auch nicht realisierbar aufgrund der

[1312] Tur v. YouTube, Inc., No. CV064436 FMC AJWX, 2007 WL 1893635, at *3.
[1313] Hendrickson v. Ebay, Inc., 165 F. Supp. 2d 1082, 1094 (C.D. Cal. 2001).
[1314] Hendrickson v. Ebay, Inc., 165 F. Supp. 2d 1082, 1094 (C.D. Cal. 2001).
[1315] Perfect 10, Inc. v. Cybernet Ventures, Inc., 213 F. Supp. 2d 1146, 1181-1182 (2002).
[1316] Perfect 10, Inc. v. Cybernet Ventures, Inc., 213 F. Supp. 2d 1146, 1181-1182 (2002).
[1317] IO Group, Inc. v. Veoh Networks, Inc., 586 F.Supp.2d 1132, 1153 (N.D.Cal. 2008); für einen solchen Ansatz auch Blevins, 34 Cardozo L. Rev. 1821, 1881 (2013).
[1318] IO Group, Inc. v. Veoh Networks, Inc., 586 F.Supp.2d 1132, 1153 (N.D.Cal. 2008).
[1319] IO Group, Inc. v. Veoh Networks, Inc., 586 F.Supp.2d 1132, 1153 (N.D.Cal. 2008).

hunderttausenden Videos, die die Nutzer des Host-Provider hochluden.[1320]

Der *Ninth Circuit* hat hingegen zunächst ausgeführt, dass sich die Möglichkeit der Kontrolle immer auf eine bestimmte rechtswidrige Handlung beziehen müsse.[1321] Dies bedeute, dass der Host-Provider, solange er keine Kenntnis eines konkreten Falles habe, er diesen auch nicht kontrollieren könne.[1322] Entsprechend urteilte das Gericht 2011, dass das Merkmal *right and ability to control* eine Kontrolle über eine spezifische rechtsverletzende Handlung, von der der Host-Provider Kenntnis hat, erfordere.[1323]

Nachdem der *Second Circuit* allerdings diese Interpretation der *right and ability to control*-Bestimmung des *Ninth Circuit* zurückwies, mit der Begründung, dass hierdurch lediglich die Bestimmung des § 512 (c) (1) (A) DMCA dupliziert werde[1324], hat auch der *Ninth Circuit* seine Urteilsbegründung[1325] aufgehoben und eine abweichende Begründung[1326] eingereicht, die diese ersetzt. Darin schließt er sich der Begründung des *Second Circuit* an und führt aus, dass der Host-Provider eine erhebliche Beeinflussung auf die Aktivitäten seiner Nutzer ausüben muss, um eine Möglichkeit zur Kontrolle zu bejahen.[1327] Eine solche erhebliche Beeinflussung sei denkbar, wenn der Host-Provider ein hohes Grad an Kontrolle über die Aktivitäten ausübe wie in *Perfect 10 v. Cybernet*[1328] oder ein zielgerichtetes Verhalten im Rahmen der *inducement*

[1320] IO Group, Inc. v. Veoh Networks, Inc., 586 F.Supp.2d 1132, 1153 (N.D.Cal. 2008).
[1321] UMG Recordings, Inc. v. Shelter Capital Partners, 667 F.3d 1022, 1042 (9th Cir. 2011).
[1322] UMG Recordings, Inc. v. Shelter Capital Partners, 667 F.3d 1022, 1042 (9th Cir. 2011); so auch Viacom Intern. Inc. v. YouTube, Inc., 718 F.Supp.2d 514, 527 (S.D.N.Y. 2010).
[1323] UMG Recordings, Inc. v. Shelter Capital Partners, 667 F.3d 1022, 1043 (9th Cir. 2011).
[1324] Viacom Intern., Inc. v. YouTube, Inc., 676 F.3d 19, 36 (2nd Cir. 2012).
[1325] UMG Recordings, Inc. v. Shelter Capital Partners, 667 F.3d 1022 (9th Cir. 2011).
[1326] UMG Recordings, Inc. v. Shelter Capital Partners, 718 F.3d 1006 (9th Cir. 2013).
[1327] UMG Recordings, Inc. v. Shelter Capital Partners, 718 F.3d 1006, 1030 (9th Cir. 2013); siehe auch Viacom Intern., Inc. v. YouTube, Inc., 676 F.3d 19, 38 (2nd Cir. 2012).
[1328] Siehe Perfect 10, Inc. v. Cybernet Ventures, Inc., 213 F.Supp.2d 1146 (C.D. California 2002).

liability[1329] aufzeige.[1330] Zudem hätten andere Gerichte angedeutet, dass eine Kontrollmöglichkeit bejaht werden könnte in Fällen in denen der Host-Provider aktiv in die Auflistung, die Versteigerung, den Verkauf und die Lieferung der von Dritten angebotenen Produkte involviert ist oder durch Vorabprüfung der Produkte, Bearbeitung der Produktbeschreibung oder dem Vorschlagen von Preisen.[1331] Dass es einer spezifischen Kenntnis bezogen auf eine konkrete Rechtsverletzung bedarf, findet sich in der geänderten Urteilsbegründung aber nicht wieder.

In *Columbia v. Fung* bejaht der *Ninth Circuit* schließlich das Merkmal der *right and ability to control*, da der Host-Provider die auf seiner Webseite gespeicherten Dateien mithilfe eines Programms organisierte, das die Dateien spezifischen Suchbegriffen zuordnete, welche Beschreibungen enthielten, die auf urheberrechtswidriges Material hinwiesen.[1332] Zudem verhalf er seinen Nutzern, persönlich urheberrechtswidriges Material ausfindig zu machen.[1333] Dies zeige den erheblichen Einfluss des Host-Providers auf die durch seine Nutzer durchgeführten rechtswidrigen Handlungen auf.[1334]

(4) Bewertung

Zuzustimmen ist der Rechtsprechung, sofern sie für eine Bejahung der Kontrolle mehr verlangt als die bloße Möglichkeit, das Material zu sperren oder zu entfernen. Dies verdeutlicht auch die Gesetzgebungsgeschichte. Während im Hinblick auf eine alte Version des DMCA und dem Ausdruck *right and ability to control* noch Bezug genommen wurde auf den *vicarious liability*-Standard,

[1329] Siehe zur *inducement liability* näher D.II.1.b)cc).
[1330] UMG Recordings, Inc. v. Shelter Capital Partners, 718 F3d 1006, 1030 (9th Cir. 2013); siehe auch Viacom Intern., Inc. v. YouTube, Inc., 676 F.3d 19, 38 (2nd Cir. 2012).
[1331] UMG Recordings, Inc. v. Shelter Capital Partners, 718 F.3d 1006, 1030 (9th Cir. 2013); siehe auch Viacom Intern., Inc. v. YouTube, Inc., 676 F.3d 19, 38 n. 13 (2nd Cir. 2012).
[1332] Columbia Pictures Industries, Inc. v. Fung, 710 F.3d 1020, 1046 (9th Cir. 2013).
[1333] Columbia Pictures Industries, Inc. v. Fung, 710 F.3d 1020, 1046 (9th Cir. 2013).
[1334] Columbia Pictures Industries, Inc. v. Fung, 710 F.3d 1020, 1046 (9th Cir. 2013).

wurde in den darauf folgenden Reports der Bezug zur *vicarious liability* ausgelassen.[1335] Der Standard ist folglich enger als bei der *vicarious liability*. Die Schlussfolgerung des *C.D. California* in *Tur v. YouTube* scheint vor diesem Hintergrund allerdings fragwürdig. Denn dass eine Kontrolle eine vorangehende Möglichkeit zur Begrenzung oder Filterung von urheberrechtlich geschützten Inhalten voraussetzt stützt das Gericht auf zwei alte Gerichtsentscheidungen, welche jeweils bzgl. der *vicarious liability* ergangen sind.[1336]

Richtigerweise wird jedenfalls, wie der *Second* und *Ninth Circuit* im Hinblick auf die Kontrollmöglichkeit im Rahmen der *vicarious liability* ausführen, *something more* gefordert.[1337] Was genau dieses *something more* ist, wird anhand des jeweiligen Einzelfalls zu bestimmen sein. Eine Kontrollmöglichkeit liegt jedenfalls nahe, wenn der Host-Provider erheblichen Einfluss auf die Aktivitäten seiner Nutzer ausübt.

ee) Notice and Takedown-Verfahren

Nach § 512 (c) (1) (C) DMCA hat der Host-Provider nach Erhalt einer *notification* das hierin als rechtsverletzend beanspruchte Material zu entfernen oder den Zugang hierzu zu sperren. Diese Bestimmung wird auch umgangssprachlich als *Notice and Takedown*-Verfahren bezeichnet. Der Anwendungsbereich überschneidet sich teilweise mit § 512 (c) (1) (A) (iii) DMCA, welcher dem Host-Provider die Verpflichtung auferlegt, das Material nach Kenntnis zu entfernen oder den Zugang hierzu zu sperren, um weiter privilegiert zu sein.[1338]

[1335] Siehe zum Verweis auf den vicarious liability standard H.R. Rep. 105-551(I), S. 27:*"The right and ability to control language in Subparagraph (B) codifies the second element of vicarious liability."*; hierzu auch UMG Recordings, Inc. v. Shelter Capital Partners, 718 F.3d 1006, 1028 (9th Cir. 2013).

[1336] Tur v. YouTube, Inc., No. CV064436 FMC AJWX, 2007 WL 1893635, at *3, mit Bezug auf Fonovisa, Inc. v. Cherry Auction, Inc., 76 F.3d 259, 263 (9th Cir. 1996) und MGM, Inc. v. Grockster, 545 U.S. 913, 926.

[1337] UMG Recordings, Inc. v. Shelter Capital Partners, 718 F.3d 1006, 1030 (9th Cir. 2013); Viacom Intern., Inc. v. YouTube, Inc., 676 F.3d 19, 38 (2nd Cir. 2012); a.A. Ginsburg, 50 Ariz. L. Rev. 577, 601 (2008).

[1338] Siehe hierzu D.III.5.b)cc)(4).

Der Host-Provider ist zur Entfernung des Materials bzw. Sperrung des Zugangs hierzu nach § 512 (c) (1) (C) DMCA nur verpflichtet, sofern die *notification* den Anforderungen des § 512 (c) (3) DMCA entspricht.[1339] Ist diese Voraussetzung erfüllt, hat die Entfernung/Sperrung zügig (*expeditiously*) zu erfolgen. Der *House* und *Senate Report* führen diesbezüglich lediglich aus, dass es nicht möglich sei, eine spezifische Zeit festzulegen, innerhalb derer der Host-Provider das Material zu entfernen habe, da die faktischen Umstände und technischen Parameter von Fall zu Fall unterschiedlich seien.[1340] Die Gerichte haben hier entsprechend einen flexiblen Maßstab angelegt. *Weinstein* kritisiert die Möglichkeit der näheren Ausgestaltung des Begriffes *expeditiousness* durch die Gerichte, da dies zu willkürlichen und inkonsistenten Ergebnissen führen würde und dem Host-Provider entsprechend keine zuverlässigen und eindeutigen Rahmenbedingungen zur Verfügung stehen würden.[1341] Stattdessen schlägt sie zur Konkretisierung des Begriffes einen 3-stufigen Angemessenheits-Test vor, der die Verwendung der neuesten Software zur Aufspürung von rechtsverletzenden Inhalten durch den Host-Provider voraussetzt und daneben die Besonderheiten der spezifischen *notification* sowie die hiermit dem Host-Provider auferlegte Kosten- und Ressourcen-Belastung in Erwägung ziehen soll.[1342] Ein solcher Test ist jedoch abzulehnen. Zunächst ist bereits nicht ersichtlich, warum der Host-Provider dazu verpflichtet werden sollte, eine bestimmte Software zur Aufspürung von rechtsverletzenden Inhalten einzusetzen, hat ihn doch der Rechteinhaber durch die *notification* gerade in die Lage zu versetzen, den rechtsverletzenden Inhalt aufzufinden. Zudem bietet auch die Prüfung und Bewertung auf zweiter und dritter Stufe genügend Ermessens- und Entscheidungsspielraum, so dass nicht

[1339] Siehe hierzu D.III.5.b)ee)(2).
[1340] H.R. Rep. 105-551(I), S. 53; S. Rep. 105-190, S. 44.
[1341] Weinstein, 26 Cardozo Arts & Ent. L.J. 598, 604 (2008).
[1342] Weinstein, 26 Cardozo Arts & Ent. L.J. 598, 609 ff. (2008).

davon auszugehen ist, dass hierdurch mehr Rechtssicherheit erlangt wird.

In *IO Group v. Veoh* hat der *N.D. California* die Löschung innerhalb eines Tages nach Erhalt der *notification* sowie innerhalb weniger Tage nach Erhalt der *notification* als genügend angesehen.[1343] Auch der *S.D.N.Y.* führte aus, dass eine Reaktion innerhalb von einem Tag nach Erhalt der *notification* dem Erfordernis der Zügigkeit genüge, hielt allerdings auch einen Zeitraum von 3,5 Wochen als ausreichend für eine *notification*, welche insgesamt 170 urheberrechtswidrig eingestellte Videos beinhaltete.[1344]

Derzeit anhängig ist ein Verfahren vor dem *D.C. Delaware*, in welchem eine Jury die Frage zu beantworten hat, ob die Löschung von einem Video innerhalb von 2 Tagen als *expeditious* i.S.d. § 512 (c) (1) (C) DMCA anzusehen ist.[1345] Das Gericht wies hier den Antrag der Beklagten auf *summary judgement*[1346] zurück.[1347] Es liege kein Präzedenzfall vor, der eine vergleichbare Sachlage behandele.[1348] Daher müsse im Rahmen eines ordnungsgemäßen Verfahrens anhand tatsächlicher Feststellungen im konkreten Fall ermittelt werden, ob die Löschung des Materials e*xpeditiously* erfolgte.[1349] Die Besonderheit liegt in diesem Fall darin, dass das beanstandete rechtsverletzende Material den Live-Stream eines pay-per-view Kampfes betrifft. Dies sah das Gericht als Grund an, genauer untersuchen zu lassen, was die Beklagte innerhalb der 48 Stunden zwischen Erhalt der *notification* und Löschung des Materials unternahm.[1350] Es bleibt abzuwarten, ob das Gericht die

---

[1343] IO Group, Inc. v. Veoh Networks, Inc., 586 F.Supp.2d 1132, 1150 (N.D.Cal. 2008).
[1344] Capitol Records, LLC v. Vimeo, LLC, 972 F.Supp. 2d 500, 536 (S.D.N.Y. 2013).
[1345] Square Ring, Inc. v. UStream.com, 2015 WL 307840 (D. Del. Jan. 23, 2015).
[1346] Zum Begriff des *summary judgements* siehe S. 353.
[1347] Square Ring, Inc. v. UStream.com, 2015 WL 307840 at *4 (D. Del. Jan. 23, 2015).
[1348] Square Ring, Inc. v. UStream.com, 2015 WL 307840 at *4 (D. Del. Jan. 23, 2015).
[1349] Square Ring, Inc. v. UStream.com, 2015 WL 307840 at *4 (D. Del. Jan. 23, 2015).
[1350] Square Ring, Inc. v. UStream.com, 2015 WL 307840 at *4 (D. Del. Jan. 23, 2015).

Tatsache, dass es sich um die Verletzung der Urheberrechte an einem Live-Stream handelte, als rechtserheblich ansieht. Vor dem Hintergrund der im *House* und *Senate Report* erwähnten erforderlichen Bewertung der faktischen Umstände, ist dies nicht auszuschließen.

Es wird bzgl. des Merkmals folglich auf die jeweiligen Umstände des Einzelfalls ankommen, i.d.R. dürfte eine Reaktion innerhalb weniger Tage dem Erfordernis der Zügigkeit aber genügen.

Die *notification* entfaltet ihre Wirkung zudem nur hinsichtlich solchen Materials, das zu dem Zeitpunkt des Empfangs der *notification* auf dem Dienst des Host-Providers vorhanden war.[1351] Eine zukunftsgerichtete Verpflichtung des Host-Providers würde diesem Monitoring-Maßnahmen auferlegen, was das vom Kongress durch die Regelungen des DMCA hergestellte Gleichgewicht stören würde.[1352] Der *C.D. California* führt diesbezüglich aus, dass es nicht die Absicht des Kongresses gewesen sei, es dem Urheberrechtsinhaber zu ermöglichen, dem Host-Provider eine Art Pauschal-*notification* zukommen zu lassen, um ihn damit von jeglicher Verantwortlichkeit zu befreien und die Verpflichtung zur Aufdeckung und Entfernung des urhebeberrechtsverletzenden Materials auf ewig dem Host-Provider aufzuerlegen.[1353]

(1) Benannter Bevollmächtigter - Designated agent

Gem. § 512 (c) (2) DMCA gelten die Haftungsprivilegien für Host-Provider nur, sofern dieser einen Bevollmächtigten bestimmt hat, an den die *notifications* zu senden sind (*designated agent*). Der Host-Provider hat gem. § 512 (c) (2) (A) DMCA im Wesentlichen folgende Informationen des *designated agents* sowohl innerhalb seines Dienstes, einschließlich seiner Webseite, öffentlich zugänglich zu machen sowie dem *Copyright Office*[1354] zur Verfügung zu stellen: Name, Adresse, Telefonnummer, E-Mail-

[1351] Hendrickson v. Amazon.com, Inc., 298 F.Supp.2d 914, 917 (C.D.Cal. 2003); Ballon, 4.12[9][B].
[1352] Hendrickson v. Amazon.com, Inc., 298 F.Supp.2d 914, 917 (C.D.Cal. 2003).
[1353] Hendrickson v. Amazon.com, Inc., 298 F.Supp.2d 914, 917 (C.D.Cal. 2003).
[1354] U.S. Copyright Office, http://www.copyright.gov.

Adresse sowie andere Kontaktinformationen, welche der sog. *Register of Copyrights*[1355] für erforderlich hält.

Nach Auffassung des *C.D. California* ist die Benennung einer natürlichen Person nicht erforderlich, es genügt bspw. auch die Angabe einer zuständigen Abteilung innerhalb des Unternehmens.[1356]

Gem. § 512 (c) (2) (B) DMCA unterhält der *Register of Copyrights* ein Verzeichnis der *agents*, welches für die Öffentlichkeit, auch im Internet, einsehbar ist. Er hat das Recht, von dem Host-Provider für die Unterhaltung dieses Verzeichnisses die Zahlung einer Gebühr zu verlangen.[1357]

(2) Notification

Die formalen Anforderungen der *notification*, damit diese wirksam ist, sind in § 512 (c) (3) DMCA festgelegt. Danach muss die *notification* als schriftliche Mitteilung an den *designated agent* gerichtet werden und im Wesentlichen (*substantially*) die bestimmte Angaben enthalten. Die *notification* wird i.d.R. per Email versendet, denkbar ist aber auch die Zusendung per Fax oder Post.

Unklar ist, warum sich der Gesetzgeber lediglich für eine im Wesentlichen die Angaben enthaltene *notification* entschieden hat und was dieser Begriff genau bedeutet. Der *House* und *Senate Report* führen hierzu aus, dass der Standard an dem die *notification* gemessen wird, der einer Compliance im Wesentlichen ist.[1358] Dieser Standard der wesentlichen Übereinstimmung soll so angewandt werden, dass technische Fehler, wie bspw. Rechtschreibfehler im Namen oder die Angabe einer veralteten Postleitzahl, sofern die Telefonnummer mit einer korrekten

[1355] Der Register of Copyrights ist der Direktor des U.S. Copyright Office gem. 17 U.S.C. § 701.
[1356] Hendicksonv. eBay, Inc., 165 F. Supp. 2d 1082, 1092 Fn. 13 (C.D. Cal. 2001).
[1357] Derzeit $ 105 Basic Filing Fee.
[1358] H.R. Rep. 105-551(II), S. 55; S. Rep. 105-190, S. 46: *„The standard against which a notification is to be judged, is one of substantial compliance."*

Adresse angegeben wurde, den Rechteinhaber nicht automatisch im Rahmen dieser Regelung disqualifizieren.[1359]

Der *Fourth Circuit* hat diesbezüglich in einem frühen Urteil ausgeführt, dass *substantial compliance* keine Perfektion voraussetze.[1360] *Schachter* zieht zur Auslegung zudem die *substantial performance*-Doktrin des Vertragsrechts heran, welche besagt, dass eine Leistung selbst dann als erfüllt angesehen wird, wenn die Leistungserfüllung nicht präzise den Bestimmungen des Vertrages entspricht, sofern sie in gutem Glauben erfolgte und der wesentliche Zweck erreicht wird.[1361] Der wesentliche Zweck der in § 512 (c) (3) DMCA aufgeführten Angaben der *notification* sei es, den Host-Provider auf urheberrechtsverletzende Inhalte aufmerksam zu machen um dadurch sicherzustellen, dass dieses gelöscht wird.[1362] Deshalb seien die notwendigen Angaben einer *notification* von den Gerichten so auszulegen, dass diesbezüglich keine Perfektion verlangt werden dürfte.[1363]

Die Gefahr eines solch ungewissen Standards besteht darin, dass der Host-Provider im Zweifel nach Erhalt einer *notification*, auch sofern diese fehlerhaft sein sollte, sicherheitshalber das Material löscht, um einer späteren Haftung zu entgehen, sollte ein Gericht feststellen, dass die fehlerhafte *notification* dennoch im Wesentlichen konform mit den Vorgaben des § 512 (c) (3) DMCA war.[1364]

Auszuschließen ist jedenfalls, dass durch dieses Erfordernis einer lediglich *substantial compliance* mit den Angaben des § 512 (c) (3) (A) (i) - (vi) DMCA, auf einzelne Inhalte komplett verzichtet werden könnte.[1365] Dies ergibt sich bereits aus dem nachfolgenden § 512 (c) (3) (B) (ii) DMCA, welcher genau regelt, welche Inhalte

---

[1359] H.R. Rep. 105-551(II), S. 56; S. Rep. 105-190, S. 47.
[1360] ALS Scan, Inc. v. Remarq Communities, Inc., 239 F.3d 619, 625 (4th Cir. 2001).
[1361] Schachter, 29 Cardozo Arts & Ent. L.J. 495, 516 (2011): *„[...] if a good-faith attempt to perfom does not precisely meet the terms of an agreement or statutory requirements, the performance will still be considered complete if the essential purpose is accomplished [...]“*.
[1362] Schachter, 29 Cardozo Arts & Ent. L.J. 495, 516 (2011).
[1363] Schachter, 29 Cardozo Arts & Ent. L.J. 495, 516 (2011).
[1364] Ballon, E-Commerce & Internet Law (2014-2015 Update), 8.12[9][B].
[1365] So auch Holznagel, S. 45.

fehlen dürfen, um den Host-Provider dazu anzuhalten, bei dem Absender der *notification* nachzuhaken, um die restlichen Informationen zu erhalten.

(a) Unterschrifterfordernis

Die *notification* ist mit einer handschriftlichen oder elektronischen Unterschrift von einer für den Inhaber der urheberrechtlichen Ausschließlichkeitsrechte autorisierten Person zu unterzeichnen.[1366] Es ist fraglich, was genau unter der elektronischen Unterschrift zu verstehen ist.

Nach Auffassung von *Nimmer* reicht es nicht aus, wenn in einer E-Mail innerhalb des Textes lediglich der Name des Absenders eingetippt wird.[1367] Die elektronische Unterschrift könnte eine solche im Sinne des *E-Sign Actes*[1368] sein. Danach ist eine elektronische Unterschrift *„an electronic sound, symbol, or process, attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record"*.[1369] Nach einem Urteil des *Fourth Circuit* liegt eine solche elektronische Unterschrift aber auch vor, wenn der Unterzeichner auf den „*Yes*"-Button im Rahmen eines Uploads klickt.[1370]

In der Praxis hat sich wohl die einfache Unterschrift in Textform eingebürgert.[1371] *Holznagel* macht in diesem Zusammenhang auf das Risiko einer *fake-notification*, also der Versendung einer *notification* unter falscher Identität, aufmerksam, insbesondere im Hinblick auf die einfache Unterschrift in Textform innerhalb einer E-Mail.[1372] Er verkennt hier jedoch, dass die Gefahr einer *fake-notification* nicht lediglich auf die Zulässigkeit einer einfachen Unterschrift in Textform zurückgeführt werden kann. Auch die

[1366] § 512 (c) (3) (A) (i) DMCA.
[1367] Nimmer on Copyright, § 12B.04 [B] [1].
[1368] Electronic Signatures in Global and National Commerce Act, dieser tritt allerdings erst zwei Jahre nach dem DMCA in Kraft.
[1369] 15 U.S.C. § 7006 (5).
[1370] Metro. Reg'l Info. Sys. v. Am. Home Realty Network, Inc., 722 F.3d 591, 601ff. (4th Cir. 2013); kritisch hierzu Nimmer on Copyright, § 10.03 [A] [1] [b], welcher anregt dieser Entscheidung nicht zu folgen.
[1371] Holznagel, S. 40.
[1372] Holznagel, S. 40.

handschriftliche Unterzeichnung und anschließende Versendung einer *notification* per Post birgt dieses Risiko.

(b) Bezeichnung des urheberrechtlich geschützten Werkes

Die *notification* muss ferner das urheberrechtlich geschützte Werk bezeichnen, dessen Verletzung geltend gemacht wird oder, falls mehrere urheberrechtlich geschützte Werke auf einer einzigen Webseite durch eine einzige *notification* abgedeckt werden, eine repräsentative Liste solcher Werke auf der Webseite.[1373] Als Beispiel nennen der *House* und *Senate Report* hier eine unautorisierte Jukebox im Internet, in welchem Fall eine einzelne Aufzählung jedes Musikwerkes, dessen Verletzung geltend gemacht wird, nicht notwendig ist.[1374]

So hat der *Fourth Circuit* in *ALS Scan v. RemarQ* den Verweis auf die eigene Webseite des Urheberrechtsinhabers als ausreichend angesehen, da auf dieser Webseite Urheberrechtswerke sowie Urheberrechtsinformationen zu finden waren.[1375]

(c) Bezeichnung des urheberrechtsverletzenden Materials

Weiterhin ist das Material, welches als urheberrechtsverletzend geltend gemacht wird, zu bezeichnen sowie hinreichende Informationen zu geben, damit der Host-Provider das Material auffinden kann.[1376] Dies kann beispielsweise eine Kopie oder Beschreibung des urheberrechtsverletzenden Materials sein sowie die Angabe der URL.[1377]

Der *Ninth Circuit* führte in diesem Zusammenhang aus, dass diese Voraussetzung nicht erfüllt sei, wenn der Host-Provider diese Informationen erst noch selbst aus mehreren Dokumenten heraussuchen und anschließend durch Durchsuchen eines 22.185 Seiten langen Dokumentes zusammenfügen muss.[1378] Hingegen könne es laut *C.D. California* im Falle eines urheberrechtswidrigen

---

[1373] § 512 (c) (3) (A) (ii) DMCA.
[1374] H.R. Rep. 105-551(II), S. 55; S. Rep. 105-190, S. 46.
[1375] ALS Scan, Inc. v. Remarq Communities, Inc., 239 F.3d 619, 625 (4th Cir. 2001).
[1376] § 512 (c) (3) (A) (iii) DMCA.
[1377] H.R. Rep. 105-551(II), S. 55; S. Rep. 105-190, S. 46.
[1378] Perfect 10, Inc. v. CCBill LLC, 488 F.3d 1102, 1113 (9th Cir. 2007).

Artikels auf einer Internetplattform ausreichend sein, wenn die *notification* die Information enthält, dass alle DVD's mit einem bestimmten Titel die Urheberrechte des Berechtigten verletzen, sofern sich die rechtsverletzenden DVD's zu diesem Zeitpunkt noch auf der Auktionsplattform befinden, da es hierdurch dem Host-Provider ermöglicht werde, das Material zügig aufzufinden.[1379] Etwas anderes gelte allerdings, wenn sich das Material zum Zeitpunkt des Erhaltes der *notification* noch nicht auf der Plattform befinde.[1380]

In dem Fall *Capitol Records v. MP3 Tunes* stellte sich der Sachverhalt wie folgt dar.[1381] Der Dienst des Providers bestand aus einem *online storage locker* auf der Webseite MP3tunes.com, eine Art persönliches Schließfach des Nutzers, in welchem dieser Musikdateien speichern konnte, sowie der Webseite Sideload.com, welche es den Nutzern ermöglichte nach MP3s im Internet zu suchen.[1382] Sofern der Nutzer der Suchmaschine auch ein Schließfach auf MP3tunes.com besaß, konnte er den auf Sideload.com gesuchten Song über diese Seite direkt herunterladen und in seinem Schließfach speichern.[1383] In diesem Zusammenhang wurde die Frage behandelt, ob eine *notification*, die die rechtsverletzenden Inhalte anhand von Links auf Sideload.com identifizierte, den Provider auch dazu verpflichtete, die Inhalte, welche seine Nutzer über Sideload.com in ihrem Schließfach gespeichert hatten, zu löschen. Der *S.D.N.Y.* urteilte, dass der Provider auch verpflichtet sei, diejenigen Inhalte zu löschen, welche auf die Schließfächer der Nutzer zurückführbar seien.[1384] Da der Provider jeden durch den Nutzer über Sideload.com in sein Schließfach heruntergeladenen Song nachverfolgen könne, enthalte

[1379] Hendrickson v. Amazon.com, Inc., 298 F.Supp.2d 914, 917 (C.D.Cal 2003).
[1380] Hendrickson v. Amazon.com, Inc., 298 F.Supp.2d 914, 917 (C.D.Cal 2003).
[1381] Capitol Records, Inc. v. MP3Tunes, LLC, 821 F.Supp.2d 627 (S.D.N.Y. 2011).
[1382] Capitol Records, Inc. v. MP3Tunes, LLC, 821 F.Supp.2d 627, 633 ff. (S.D.N.Y. 2011); auch *Cyberlocker* genannt.
[1383] Capitol Records, Inc. v. MP3Tunes, LLC, 821 F.Supp.2d 627, 634 (S.D.N.Y. 2011).
[1384] Capitol Records, Inc. v. MP3Tunes, LLC, 821 F.Supp.2d 627, 643 (S.D.N.Y. 2011).

die *notification* mit Angabe der Links auf Sideload.com ausreichend Informationen, die es dem Provider ermöglichten, Kopien der rechtsverletzenden Songs in den Schließfächern der Nutzer zu lokalisieren.[1385]

In dem gleichen Urteil entschied der *S.D.N.Y.* auch, dass es nicht ausreichend sei, wenn die *notification* lediglich eine repräsentative Liste der urheberrechtsverletzenden Inhalte enthalte.[1386] Dies hatte der *S.D.N.Y.* zuvor bereits in der Entscheidung *Viacom v. YouTube* erklärt.[1387] Hier führte er weiter aus, dass zwar gem. § 512 (c) (3) (A) (ii) DMCA eine repräsentative Liste ausreicht, dass der folgende § 512 (c) (3) (A) (iii) DMCA allerdings verlangt, dass das rechtsverletzende Material so identifiziert werden muss, dass es dem Host-Provider möglich ist, dass Material aufzufinden.[1388] Entsprechend genüge eine allgemeine Beschreibung, wie bspw. alle Werke eines bestimmten Künstlers, ohne Angabe der genauen Fundstelle, nicht aus, um den Host-Provider in die Lage zu versetzen, die als rechtsverletzend geltend gemachten Inhalte aufzufinden.[1389] Der *C.D. California* zeigte diesbezüglich in *UMG Recordings v. Veoh Networks* auf, dass lediglich die Nennung eines Künstlers ohne weitergehende Informationen zur genauen Lokalisierung, zu der unerwünschten Folge von *false positives*, also dem Anzeigen von zulässigen Inhalten, führen kann.[1390]

Dem Ergebnis ist zuzustimmen.[1391] Dass es nicht ausreichend ist, eine lediglich repräsentative Liste der als rechtsverletzend geltend gemachten Inhalte einzureichen, ergibt sich allerdings bei genauer Betrachtung auch daraus, dass die repräsentative Liste gesetzlich

---

[1385] Capitol Records, Inc. v. MP3Tunes, LLC, 821 F.Supp.2d 627, 643 (S.D.N.Y. 2011).
[1386] Capitol Records, Inc. v. MP3Tunes, LLC, 821 F.Supp.2d 627, 643 (S.D.N.Y. 2011).
[1387] Viacom Intern. Inc. v. YouTube, Inc., 718 F.Supp.2d 514, 529 (S.D.N.Y. 2010).
[1388] Viacom Intern. Inc. v. YouTube, Inc., 718 F.Supp.2d 514, 529 (S.D.N.Y. 2010).
[1389] Viacom Intern. Inc. v. YouTube, Inc., 718 F.Supp.2d 514, 528 ff. (S.D.N.Y. 2010).
[1390] UMG Recordings, Inc. v. Veoh Networks Inc., 665 F.Supp.2d 1099, 1110 (C.D. Cal. 2009).
[1391] A.A. Rasenberger/Pepe, 59 J. Copyright Soc'y U.S.A., 627, 669 f. (2012).

lediglich im Hinblick auf die Identifizierung der urheberrechtlich geschützten Werke geregelt ist und eben nicht im Hinblick auf die als urheberrechtswidrig beanstandeten zu identifizierenden Inhalte.[1392]

Entsprechend beruhen auch die Ausführungen des *Fourth Circuit* in *ALS Scan v. Remarq* auf einem falschen Verständnis, sofern dieser ausführt, dass das Erfordernis einer lediglich repräsentativen Liste, dem Urheberrechtsinhaber nicht die Last auferlegen soll, jedes einzelne rechtsverletzende Werk zu identifizieren.[1393]

(d) Angabe von Kontaktdaten

Die *notification* muss ausreichende Informationen enthalten, um dem Host-Provider die Kontaktaufnahme mit der Beschwerde führenden Partei zu ermöglichen, wie bspw. Adresse, Telefonnummer und E-Mail Adresse.[1394]

(e) Erklärung nach gutem Glauben

Der *notification* ist zudem eine Erklärung beizufügen, dass die Beschwerde führende Partei im guten Glauben davon ausgeht, dass die Nutzung des beanstandeten Materials nicht durch den Urheberrechtsinhaber, seinen Bevollmächtigtem oder durch Gesetz autorisiert ist.[1395] Nicht Inhalt der *notification* sind folglich materiell-rechtliche Ausführungen hinsichtlich der behaupteten Rechtsverletzung.

In *Rossi v. MPAA* führte der *Ninth Circuit* diesbezüglich aus, dass bei der Bestimmung, ob der Absender der *notification* in gutem Glauben gehandelt hat, ein subjektiver und kein objektiver Maßstab anzulegen sei.[1396] Obwohl kein anderes Gericht bislang die Bedeutung des guten Glaubens im Rahmen des DMCA interpretiert

---

[1392] § 512 (c) (3) (A) (ii) DMCA behandelt die Auflistung der urheberrechtlich geschützten Werke, während § 512 (c) (3) (A) (iii) DMCA die Auflistung der urheberrechtswidrigen Werke behandelt.

[1393] ALS Scan, Inc. v. Remarq Communities, Inc., 239 F.3d 619, 625 (4th Cir. 2001); einem entsprechend falschen Verständnis erliegt auch Mazoki, 30 Tem. J. Sci. Tech. & Envtl. 275, 300 (2011).

[1394] § 512 (c) (3) (A) (iv) DMCA.

[1395] § 512 (c) (3) (A) (v) DMCA.

[1396] Rossi v. Motion Picture Ass'n of America Inc., 391 F.3d 1000, 1004 (9th Cir. 2004).

habe, könne auf die traditionelle Interpretation dieses Begriffs im Rahmen anderer Bundesgesetze zurückgegriffen werden.[1397] Dies ergebe sich auch aus dem Gesamtgefüge des § 512 DMCA, insbesondere vor dem Hintergrund, dass § 512 (f) DMCA eine Haftung aufgrund falscher Angaben in einer *notification* lediglich für den Fall vorsehe, dass der Absender wissentlich falsche Angaben macht (*knowingly misrepresents*).[1398] Eine Haftung aufgrund eines unwissentlichen Fehlers, auch sofern dieser auf einer unangemessenen oder unbilligen Handlung des Absenders basiere, sei ausgeschlossen.[1399] Erforderlich sei für die Haftung wegen falscher Angaben in der *notification* vielmehr die tatsächliche Kenntnis über die falsche Angabe.[1400] Stelle man folglich die Bestimmung hinsichtlich des guten Glaubens und die Bestimmung hinsichtlich der Haftung für falschen Angaben gegenüber, so ergebe sich hieraus ein gesetzliches Gefüge, dass die Haftung des Absenders einer *notification* davon abhängig mache, dass dieser wissentlich falsche Angaben mache.[1401] Potentielle Urheberrechtsverletzer sollen hierdurch von subjektiv missbräuchlichen Handlungen des Rechtsinhabers geschützt werden.[1402]

Entsprechend urteilte der *Ninth Circuit*, dass der Urheberrechtsinhaber in dem zu bewertenden Fall in gutem Glauben gehandelt habe.[1403] Nachdem ein Mitarbeiter der Anti-Piracy Abteilung des Urheberrechtsinhabers auf die Webseite mit dem vermeintlich rechtsverletzenden Inhalten hingewiesen wurde,

[1397] Rossi v. Motion Picture Ass'n of America Inc., 391 F.3d 1000, 1004 (9th Cir. 2004).
[1398] Rossi v. Motion Picture Ass'n of America Inc., 391 F.3d 1000, 1004 f. (9th Cir. 2004).
[1399] Rossi v. Motion Picture Ass'n of America Inc., 391 F.3d 1000, 1005 (9th Cir. 2004).
[1400] Rossi v. Motion Picture Ass'n of America Inc., 391 F.3d 1000, 1005 (9th Cir. 2004).
[1401] Rossi v. Motion Picture Ass'n of America Inc., 391 F.3d 1000, 1005 (9th Cir. 2004).
[1402] Rossi v. Motion Picture Ass'n of America Inc., 391 F.3d 1000, 1005 (9th Cir. 2004).
[1403] Rossi v. Motion Picture Ass'n of America Inc., 391 F.3d 1000, 1006 (9th Cir. 2004).

überprüfte dieser Mitarbeiter die Webseite.[1404] Durch Aussagen auf der Website wie „Join to download full length movies online now! new movies every month“, „Full Length Downloadable Movies“ und „NOW DOWNLOADABLE“, schloss der Mitarbeiter in gutem Glauben darauf, dass Filme des Urheberrechtsinhabers zum Download auf der Webseite bereitgehalten werden würden.[1405] Diese Schlussfolgerung würde die eindeutige Sprache auf der Webseite einem geradezu aufzwingen.[1406] Das Gericht sah es daher nicht als notwendig an, diesbezüglich weitere Untersuchungen anzustellen oder zu versuchen Filme, tatsächlich von der Seite herunterzuladen.[1407]

Diese Schlussfolgerung ist insbesondere vor dem Hintergrund fraglich, dass gem. § 512 (3) (A) (iii) DMCA das Material, welches vermeintlich Urheberrechte verletzt, identifiziert werden muss. Es ist unklar, wie eine solche Identifizierung stattfinden soll, wenn der Urheberrechtsinhaber selbst eine entsprechende Identifizierung nicht vornimmt. Zwar ist es gerechtfertigt hier einen subjektiven Standard anzusetzen, der danach fragt, ob der Urheberrechtsinhaber subjektiv in gutem Glauben gehandelt hat. Dies kann sich aber nur auf den guten Glauben des tatsächlich vorgefundenen Materials und dessen urheberrechtsverletzende Natur beziehen und nicht darauf, dass der Absender der *notification* in guten Glauben davon ausgeht, dass Material überhaupt erst vorhanden ist.

Bei der Frage ob der Absender einer *notification* in gutem Glauben handelte, ist somit richtigerweise auf die subjektive Kenntnis des Absenders abzustellen. Dabei hat er sicherzustellen, dass urheberrechtsverletzendes Material überhaupt existiert.[1408]

[1404] Rossi v. Motion Picture Ass'n of America Inc., 391 F.3d 1000, 1005 (9th Cir. 2004).
[1405] Rossi v. Motion Picture Ass'n of America Inc., 391 F.3d 1000, 1005 (9th Cir. 2004).
[1406] Rossi v. Motion Picture Ass'n of America Inc., 391 F.3d 1000, 1005 (9th Cir. 2004).
[1407] Rossi v. Motion Picture Ass'n of America Inc., 391 F.3d 1000, 1003 f. (9th Cir. 2004).
[1408] So im Endeffekt auch der *Ninth Circuit* in seinem späteren Urteil Lenz v. Universal Music Corp., 801 F.3d 1126, 1135 (9th Cir. 2015), in welchem er ausführt, dass der DMCA voraussetzt, dass der Urheberrechtsinhaber das Material vor Versendung der *notifcation* betrachtet: „*The DMCA already*

(f) Korrektheit der Angaben

Zudem muss die *notification* eine eidesstattliche Erklärung beinhalten (*under penalty of perjury*), dass die hierin gemachten Informationen korrekt sind und dass die Beschwerde führende Partei berechtigt ist, im Namen des Inhabers der urheberrechtlichen Ausschließlichkeitsrechte zu handeln.[1409]

(3) Folgen einer unvollständigen Notification

Eine *notification*, welche nicht im Wesentlichen mit diesen Anforderungen übereinstimmt, kann gem. § 512 (c) (3) (B) (i) DMCA nicht unter § 512 (1) (A) DMCA herangezogen werden, um zu bestimmen, ob ein Host-Provider *actual knowledge* oder *awareness* bezüglich einer rechtswidrigen Handlung hat.

Für den Fall, dass die *notification* nicht im Wesentlichen mit den Anforderungen des § 512 (c) (3) (A) DMCA übereinstimmt, aber im Wesentlichen mit den Ziffern (ii), (iii) und (iv) dieses Absatzes, findet § 512 (c) (3) (B) (i) DMCA nur Anwendung, sofern der Host-Provider umgehend versucht hat, die Person zu kontaktieren, von der die *notification* stammt oder sonstige angemessene Maßnahmen ergreift, um den Erhalt einer *notification*, welche im Wesentlichen mit § 512 (c) (3) (A) DMCA übereinstimmt, zu unterstützen.[1410]

Dies bedeutet, dass es ausreicht, wenn der Host-Provider eine *notification* erhält, welche lediglich das urheberrechtlich geschützte Material und das beanstandete urheberrechtsverletzende Material, inklusive des genauen Fundortes, bezeichnet sowie ausreichende Kontaktdaten der Beschwerde führenden Partei enthält. Unternimmt der Host-Provider anschließend ausreichende Bemühungen, um eine *notification* zu erhalten, welche die restlichen gesetzlichen Angaben erhält, ist er weiterhin privilegiert.

---

requires copyright owners to make an initial review of the potentially infringing material prior sending a takedown notice [...]"; siehe hierzu näher D.III.5.i)aa).

[1409] § 512 (c) (3) (A) (vi) DMCA.

[1410] § 512 (c) (3) (B) (ii) DMCA.

(4) Benachrichtigung des behaupteten Rechtsverletzers

Gem. § 512 (g) (2) (A) DMCA hat der Host-Provider umgehend angemessene Schritte zu unternehmen, um den *subscriber* über die Entfernung bzw. Blockierung seines Materials zu informieren, sofern er sich auf die Haftungsfreistellung hinsichtlich der Entfernung bzw. Sperrung des Materials aufgrund der *notification* berufen will. Dies beinhaltet bspw. das Versenden einer E-Mail an eine E-Mail Adresse, welche dem geposteten Material zugeordnet ist, oder welche der *subscriber* im Zusammenhang mit seinem Abonnement angegeben hat.[1411] Der Host-Provider ist nicht dazu verpflichtet, außerhalb seiner Aufzeichnungen nach Kontaktdaten des *subscribers* zu suchen.[1412] Hat der *subscriber* falsche Angaben ggü. dem Host-Provider gemacht, so ist der Host-Provider nicht dafür verantwortlich, wenn die Information bzgl. der Löschung bzw. Sperrung nicht den *subscriber* erreicht.[1413]

(5) Abweichungen von dem gesetzlich vorgegebenen System

Die Struktur des *notification*-Systems ist von dem ISP einzuhalten. Abweichungen können ihm den Schutz des DMCA *safe harbor* verwehren. So hat der *C.D. California* in einem Fall ausgeführt, dass eine Policy, welche bestimmt, dass der Rechteinhaber sämtliche gesetzlichen Anforderungen an eine *notification* erfüllen muss, ohne dass eine Heilung gem. § 512 (c) (3) (B) (ii) DMCA möglich wäre und welche zudem nicht die Angabe einer repräsentativen Liste im Sinne des § 512 (c) (3) (A) (ii) DMCA zulässt, die gesetzgeberisch ausgewogene Lastenverteilung zwischen Rechteinhaber und ISP derart zu Ungunsten des Rechteinhaber verschiebt, dass der ISP kein funktionierendes *notification*-System implementiert habe.[1414]

[1411] H.R. Rep. 105-551(II), S. 59; S. Rep. 105-190, S. 50.
[1412] H.R. Rep. 105-551(II), S. 59; S. Rep. 105-190, S. 50.
[1413] H.R. Rep. 105-551(II), S. 60; S. Rep. 105-190, S. 50.
[1414] Perfect 10, Inc. v. Cybernet Ventures, Inc., 213 F.Supp.2d 1146, 1179 ff. (2002).

ff) Fazit

Die anfängliche Verwirrung hinsichtlich der ähnlich formulierten Standards der *vicarious liability* und der *safe harbor*-Privilegien des Host-Providers scheint durch die zwischenzeitlich ergangene Rechtsprechung weitgehend ausgeräumt.[1415] Es ist mittlerweile gängige Rechtsprechung, dass die Merkmale des *direct financial benefit* und *right and ability to control* weiter auszulegen sind als im Anwendungsbereich der *vicarious liability*. Nur so wird das vom Kongress ausdrücklich beabsichtigte Ergebnis erreicht, dass sowohl Fälle der *secondary liability* als auch der *vicarious liability* in ihren Rechtsfolgen von den *safe harbor*-Privilegien begrenzt werden.

Rasenberger/Pepe sind hingegen der Auffassung, dass die Gerichte die Merkmale der Kenntnis, des finanziellen Vorteils und der Kontrollmöglichkeit zu eng ausgelegt haben und es damit zu leicht für die Host-Provider gemacht haben, sich für das *safe harbor* Privileg zu qualifizieren.[1416] Als Resultat seien selbst solche Provider einer Haftung entkommen, die sich der Tatsache bewusst waren, dass massenhaft Urheberrechtsverletzungen durch ihren Service begangen wurden und die bewusst davon profitierten oder sogar abhängig davon waren.[1417]

Dreh- und Angelpunkt für den Host-Provider bildet in der Praxis das *Notice and Takedown*-Verfahren. Auch die Gerichte sind in der Regel dazu geneigt, dem Host-Provider eine Kenntnis vornehmlich nach vorheriger Zusendung einer *notification* zuzuschreiben, auch wenn die *notification* streng gesehen gerade keine Kenntnis über die Rechtswidrigkeit eines bestimmten Materials vermittelt. Sie nimmt den Host-Provider bei Einhaltung der formellen Voraussetzungen vielmehr in die Pflicht, das Material zu entfernen oder zu sperren, ohne allerdings etwas über die materiell-rechtliche

[1415] So im Jahr 2004 noch Reese, 34 Sw. U. L. Rev. 287, 323 (2004): *„Confusion is the primary product of the DMCA thus far. [...] Much of that, however, was created by Congress' use of language that approximates contributory and vicarious liability."*

[1416] Rasenberger/Pepe, 59 J. Copyright Soc'y U.S.A. 627, 667 (2012).

[1417] Rasenberger/Pepe, 59 J. Copyright Soc'y U.S.A. 627, 667 (2012).

Begründetheit der darin geltend gemachten Urheberrechtsverletzung auszusagen. Aus diesem Grund ist auch *Holznagel* nicht zu folgen, sofern dieser aus § 512 (g) DMCA und der darin enthaltenen *good faith*-Bestimmung darauf schließt, dass der Host-Provider nicht in Kenntnis der Unbegründetheit einer *notification* den *takedown* vornehmen darf[1418]. Dies würde gerade dem Sinn und Zweck des *Notice and Takedown*-Verfahrens widersprechen und den Host-Provider wiederum dem Risiko aussetzen, trotz Befolgung des gesetzlich vorgeschriebenen Verfahrens, den Schutz des *safe harbor* zu verlieren.

Hauptgrund der zurückhaltenden Zuschreibung einer *actual* oder *red flag knowledge* der Gerichte mag in der oftmals schwierigen Beweisführung einer solchen Kenntnis des Host-Providers liegen. Hinzu kommt, dass insbesondere bei einer Kenntnis des Host-Providers, welche dieser aufgrund eigens initiierter Überwachungsmaßnahmen erlangt, Zurückhaltung geboten ist. Diesbezüglich führt auch der *Conference Report* aus, dass die Bestimmungen des DMCA nicht dazu gedacht sind, den Host-Provider davon abzuhalten seinen Dienst auf urheberrechtsverletzendes Material hin zu untersuchen und dass die Gerichte nicht allein aus der Tatsache, dass der Host-Provider ein Überwachungsprogramm unterhält, auf dessen Verwirkung einer *safe harbor* Privilegierung schließen sollen.[1419]

Reagiert der Host-Provider auf eine formal korrekte *notification* nicht, so verliert er den Schutz der *safe harbor*-Privilegien. Allerdings bedeutet dies nicht zugleich, dass er für eine Urheberrechtsverletzung seiner Nutzer haftet.[1420] Die potentielle Haftung richtet sich dann vielmehr nach den Grundsätzen der *common law secondary liability*.

[1418] Holznagel, S. 44.

[1419] Conference Report, S. 73.

[1420] Anschaulich ausgedrückt soweit Fatwallet, Inc. v. Best Buy Enterprise Services, Inc., No. 03-C-50508, 2004 U.S. Dist. LEXIS 6153 (N.D. Ill. Apr. 12, 2004):„ *Nothing in the DMCA [...] creates liability for the ISP beyond that which already exists under copyright law generally. An ISP suffers no adverse consequences under the DMCA for its failure to abide by the notice. It is free to thumb its nose at the notice and it will suffer no penalty nor increased risk of copyright liability*“.

Wegen der mit dem derzeitigen DMCA *safe harbor* System für Host-Provider verbundenen Unzulänglichkeiten, plädieren *Helman/Parchomovsky* dafür, dieses durch einen sog. *technology safe harbor* zu ersetzen.[1421] Danach sind alle Host-Provider, die beste vorhandene Technologien (*best available technology*) einsetzen, um Urheberrechtsverletzungen ex ante herauszufiltern und automatisch zu löschen, von Schadensersatzansprüchen der Rechteinhaber freigestellt.[1422] Die Umsetzung des *technology safe harbors* soll in drei Schritten erfolgen. Zunächst soll entweder unter der Schirmherrschaft des *Copyright Offices* oder einer privaten Gesellschaft eine einzige Datenbank kreiert werden, in die Urheberrechtsinhaber sämtliche Urheberrechtswerke eintragen können.[1423] Anschließend soll das *Copyright Office* zusammen mit den verschiedenen Interessenvertretern eine Liste mit den besten verfügbaren Technologien erstellen und diese anschließend periodisch anpassen.[1424] Und schließlich sollen sog. *Filtering Clearhouses* etabliert werden, die diese Technologien anwenden, um konzentriert die Filterung aller Daten eines Host-Providers ex ante vorzunehmen.[1425] Alternativ könne der Host-Provider sich auch dazu entschließen die Filterung in-house durchzuführen.[1426]

Abgesehen von den immensen Kosten und des administrativen Aufwands zur Einrichtung eines solchen Systems, lässt es datenschutzrechtliche Gesichtspunkte sowie die Grenzen einer solchen technischen Filterung, insbesondere die Erkennung autorisierter oder gesetzlich genehmigter Inhalte, gänzlich außer Betracht. Es ist daher abzulehnen.

c) Cache-Provider

§ 512 (b) DMCA regelt die Verantwortlichkeitsprivilegierung des Cache-Providers. Hiervon erfasst ist die Speicherung von Material im Rahmen des *Caching*, um die Leistungsfähigkeit des Netzwerks

[1421] Helman/Parchomovsky, 111 Colum. L. Rev. 1194, 1195 (2011).
[1422] Helman/Parchomovsky, 111 Colum. L. Rev. 1194, 1219 (2011).
[1423] Helman/Parchomovsky, 111 Colum. L. Rev. 1194, 1219 (2011).
[1424] Helman/Parchomovsky, 111 Colum. L. Rev. 1194, 1223 f. (2011).
[1425] Helman/Parchomovsky, 111 Colum. L. Rev. 1194, 1226 (2011).
[1426] Helman/Parchomovsky, 111 Colum. L. Rev. 1194, 1226 (2011).

zu erhöhen, die Überlastung des Netzwerkes im Allgemeinen sowie die Überlastung und Verzögerungen bei populären Seiten zu reduzieren.[1427]

aa) Caching im Sinne des § 512 (b)

Der Cache-Provider ist gem. § 512 (b) (1) DMCA nicht verantwortlich *„for infringement of copyright by reason of the intermediate and temporary storage of material on a system or network controlled or operated by or for the service provider“*, sofern das Caching auf Grundlage des folgenden Vorgangs geschieht.

Das Material muss von einer anderen Person als dem Cache-Provider (Uploader) öffentlich zugänglich gemacht worden sein.[1428] Zudem muss es von dem Uploader durch das System bzw. Netzwerk des Cache-Providers an eine andere Person (Anfrager) auf deren Weisung hin übermittelt werden.[1429]

Schließlich muss die Speicherung im Rahmen eines automatischen technischen Prozesses erfolgt sein zu dem Zweck, das Material Nutzern des Systems bzw. Netzwerkes des Cache-Providers (Nutzern) zugänglich zu machen, die, nachdem das Material zuvor schon mal zwischen Uploader und Anfrager übermittelt wurde, Zugang zu dem Material bei dem Uploader anfragen.[1430]

bb) Weitere Voraussetzungen der Privilegierung

Zusätzlich zu diesen Bestimmungen, enthält § 512 (b) (2) DMCA die folgenden weiteren Voraussetzungen, die der Cache-Provider zur Inanspruchnahme der Privilegien zu erfüllen hat.

(1) Keine Veränderung des Materials

Der Inhalt des Materials darf während der Übermittlung an den Nutzer nicht geändert werden, so dass es nicht von dem ursprünglich vom Uploader übermittelten Material abweicht.[1431]

[1427] H.R. Rep. 105-551(II), S. 52; S. Rep. 105-190, S. 42.
[1428] § 512 (b) (1) (A) DMCA.
[1429] § 512 (b) (1) (B) DMCA.
[1430] § 512 (b) (1) (C) DMCA.
[1431] § 512 (b) (2) (A) DMCA.

Beispielhaft aufgeführt ist im *House* und *Senate Report*, dass der Cache-Provider nicht die Werbung, welche auf der Ursprungsseite mit dem Material verbunden ist, verändern darf.[1432] Diese Voraussetzung dient zwei unterschiedlichen Zielen.[1433] Zum einen beschützt sie den Uploader im Hinblick auf die Integrität seines online gestellten Materials.[1434] Zum anderen stellt sie sicher, dass die Tätigkeit des Cache-Providers lediglich einen neutralen, automatischen und passiven Charakter hat.[1435] Dies erklärt zudem warum die Privilegierung des Cache-Providers, im Gegensatz zum Host-Provider, nicht an die Unkenntnis eines rechtsverletzenden Materials geknüpft ist.[1436]

(2) Beachtung von Vorgaben bzgl. der Aktualisierung

Der Cache-Provider muss weiterhin die Vorgaben hinsichtlich des Aktualisierens und Neuladens des Materials beachten, die der Uploader spezifiziert hat, sofern diese dem allgemein anerkannten Industriestandard für Datenübertragungsprotokolle entsprechen und soweit diese Regeln nicht dafür genutzt werden, die Zwischenspeicherung zu verhindern oder auf unzumutbare Weise zu beeinträchtigen.[1437]

Der hier genannte anerkannte Standard ist das Hypertext Transfer Protocol (HTTP), in dessen sog. *Header* entsprechende Vorgaben durch den Uploader eingebaut werden können.[1438] Dies können bspw. Vorgaben dahingehend sein, dass der Cache-Provider bei jedem Abruf durch einen Nutzer die originäre Seite des Uploaders zunächst zu Validierungszwecken kontaktieren muss, bevor er anschließend das Material an den Nutzer übermittelt, dass eine spezifische Zeitspanne festgelegt wird, innerhalb derer das Material als aktuell angesehen wird oder aber dass bestimmte Elemente durch den Cache-Provider erst gar nicht zwischengespeichert

[1432] H.R. Rep. 105-551(II), S. 52; S. Rep. 105-190, S. 43.
[1433] Peguera, 56 J. Copyright Soc'y U.S.A. 589, 607 (2009).
[1434] Peguera, 56 J. Copyright Soc'y U.S.A. 589, 607 (2009).
[1435] Peguera, 56 J. Copyright Soc'y U.S.A. 589, 607 (2009).
[1436] Peguera, 56 J. Copyright Soc'y U.S.A. 589, 607 (2009).
[1437] § 512 (b) (2) (B) DMCA.
[1438] Peguera, 56 J. Copyright Soc'y U.S.A. 589, 608 (2009).

werden dürfen.[1439] Anhand dieser Vorgaben ist der Cache-Provider in der Lage zu beurteilen, ob die zwischengespeicherten Materialien als aktuell angesehen werden können oder ob eine Überprüfung mit der originären Seite des Uploaders erforderlich ist.[1440]

Um zu verhindern, dass dem Cache-Provider hierdurch für ihn unzumutbare Maßnahmen auferlegt werden, bspw. dass der Cache-Provider jede Millisekunde zu aktualisieren hat, wurde der letzte Halbsatz eingebaut, der solche unbilligen Beeinträchtigungen untersagt.[1441]

(3) Keine Beeinträchtigung des Erhalts bestimmter Informationen

Zudem darf die Anwendung von Technologien, welche mit dem Material verbunden sind und durch welche der Uploader bestimmte Informationen erhält, durch den Cache-Provider nicht beeinträchtigt werden.[1442] Der *House* und *Senate Report* nennt hier als Beispiel sog. *hit counts*, also die Zählung von Zugriffen auf das Material.[1443] Diese Technologie muss allerdings die folgenden drei Voraussetzungen erfüllen. Zum einen darf die Technologie nicht wesentlich die Leistung des Systems bzw. Netzwerkes des Cache-Providers oder die Zwischenspeicherung des Materials beeinträchtigen.[1444] Zum anderen muss die Technologie dem allgemein anerkannten Industriestandard für Datenübertragungsprotokolle entsprechen.[1445] Ob ein entsprechender Standard überhaupt existiert, ist zweifelhaft. Der *Conference Report* führt an, dass sich diese Standards gerade erst in der ersten Entwicklungsphasen befänden und davon ausgegangen werde, dass die Normungsorganisationen der Internetindustrie, wie bspw. die *Internet Engineering Task Force*

[1439] Peguera, 56 J. Copyright Soc'y U.S.A. 589, 608 (2009).
[1440] Peguera, 56 J. Copyright Soc'y U.S.A. 589, 608 (2009).
[1441] Nimmer on Copyright, § 12B.03 [A] [1].
[1442] § 512 (b) (2) (C) DMCA.
[1443] H.R. Rep. 105-551(II), S. 52; S. Rep. 105-190, S. 43.
[1444] § 512 (b) (2) (C) (i) DMCA.
[1445] § 512 (b) (2) (C) (ii) DMCA.

oder das *World Wide Web Consortium*, zeitnah und ohne Verzögerungen agieren werden, um solche Protokolle zu entwickeln.[1446] Bis heute ist dies offensichtlich nicht geschehen, weshalb die genaue Bedeutung dieser Voraussetzung noch immer unklar ist.[1447] Schließlich darf die Technologie nicht weitere Informationen aus dem System bzw. Netzwerk des Cache-Provider extrahieren als diese, die der Uploader erhalten hätte, hätte der Nutzer den Zugang zu dem Material direkt auf der Seite des Uploaders erlangt.[1448]

(4) Beachtung von Zugangsbedingungen

Falls der Uploader für den Zugang zu dem Material bestimmte Bedingungen festgelegt hat, beispielsweise die Zahlung einer Gebühr oder die Eingabe eines Passwortes, so muss auch der Cache-Provider den Zugang zu dem Material an diese Bedingungen knüpfen.[1449] Hierdurch soll die Umgehung der von dem Uploader gesetzten Bedingungen durch die Zwischenschaltung des Cache-Providers verhindert werden.[1450]

(5) Unverzügliche Entfernung/Sperrung

Als letzte Voraussetzung hat der Cache-Provider unverzüglich zu handeln und das Material zu entfernen bzw. den Zugang hierzu zu sperren, sofern der Uploader das Material ohne Zustimmung des Urheberrechtsinhabers online gestellt hat und der Cache-Provider diesbezüglich eine *notification* gemäß § 512 (c) (3) DMCA erhalten hat.[1451] Da die Zwischenspeicherung des Cache-Providers allerdings automatisch erfolgt, gilt dies nur, sofern das Material auch auf der Ursprungsseite entfernt bzw. gesperrt wurde oder wenn eine entsprechende gerichtliche Anordnung vorliegt und die *notification* eine Erklärung enthält, durch welche bestätigt wird, dass das Material auf der Ursprungsseite entfernt bzw. gesperrt

[1446] Conference Report, S. 73.
[1447] Nimmer on Copyright, § 12B.03 [A] [1].
[1448] § 512 (b) (2) (C) (iii) DMCA.
[1449] § 512 (b) (2) (D) DMCA.
[1450] Peguera, 56 J. Copyright Soc'y U.S.A. 589, 609 (2009).
[1451] § 512 (b) (2) (E) DMCA.

wurde oder das eine entsprechende gerichtliche Anordnung vorliegt.[1452] Eine Benachrichtigung des Nutzers nach § 512 (g) (2) (A) DMCA durch den Cache-Provider ist nicht erforderlich.[1453] Dies ergibt sich bereits aus der Tatsache dass § 512 (g) (2) DMCA nach dem Wortlaut lediglich im Hinblick auf *material residing at the direction of a subscriber* anwendbar ist. Auch die Möglichkeit einer *counter notification*[1454] des betroffenen Inhalteanbieters sowie eines *put back*-Verfahrens[1455] ist nicht gegeben.

cc) Einschlägige Rechtsprechung

Es gibt bislang kaum Rechtsprechung zu § 512 (b) DMCA. Lediglich ein Fall behandelt den *safe harbor* des Cache-Providers und erörtert in diesem Zusammenhang, allerdings recht lapidar, einen Teil der Voraussetzungen.[1456] Leider erweist sich diese Anwendung des § 512 (b) DMCA bei näherer Betrachtung zudem als falsch.[1457]

Der Fall behandelte die von Google eingesetzten *Googlebots*, die das gesamte Internet absuchen und sämtliche Webseiten und deren Inhalte im Google Cache zwischenspeichern. Führt der Google-Nutzer nun eine Suchanfrage durch, so kann er sich die Suchergebnisse durch Anklicken des Google Cache-Links auch in der im Cache gespeicherten Seite anzeigen lassen und nicht auf der aktiven Webseite.[1458]

Der *District Court of Nevada* hat in seiner Urteilsbegründung ausgeführt, dass Google die Voraussetzungen des § 512 (b) (1) (B) DMCA erfülle, da der Uploader das Material auf Googles Anforderung an Googles *Googlebot* übermittelte und es sich bei

[1452] § 512 (b) (2) (E) (i) und (ii) DMCA.
[1453] So auch Urban/Quilter, 22 Santa Clara Computer & High Tech. L.J. 621, 628 (2006).
[1454] Siehe hierzu S. 333.
[1455] Siehe hierzu S. 336.
[1456] Field v. Google Inc., 412 F.Supp.2d 1106 (2006).
[1457] So auch Nimmer on Copyright, § 12B.03 [A] [2]; Peguera, 56 J. Copyright Soc'y U.S.A. 589, 645 (2009).
[1458] Eine genaue Beschreibung des Cache-Features findet sich unter https://support.google.com/websearch/answer/1687222?hl=de&ref_topic=3036132, zuletzt besucht am 24.04.2016.

Google um eine andere Person als den Uploader handele.[1459] Zudem sei die Voraussetzung des § 512 (b) (1) (C) DMCA erfüllt, da der Zweck von Googles Cache derjenige sei, ihren Nutzern Zugang zu dem angefragten Material zu verschaffen für den Fall, dass die originäre Webseite, aus welchem Grund auch immer, nicht verfügbar ist.[1460]

Dem kann nicht gefolgt werden. Die Anwendbarkeit des § 512 (b) DMCA scheitert bereits an der Voraussetzung des § 512 (b) (1) (B) DMCA.[1461] Das Material wird nämlich nicht auf Anfrage einer dritten Person an diese durch das Netzwerk des Cache-Providers geleitet. Vielmehr sucht der Cache-Provider selbst aktiv das gesamte Internet ab. Auch § 512 (b) (1) (C) DMCA erscheint problematisch, da der Nutzer Zugang zu dem Material nicht von dem ursprünglichen Uploader anfordert, sondern er sich explizit durch Anklicken des Google Cache-Links dafür entscheidet, sich die Seite im Archiv des Google Cache anzeigen zu lassen.[1462] Es fehlt hier an der vom Gesetz verlangten Vier-Personen-Konstellation.[1463]

dd) Fazit

Die Privilegierung des Cache-Providers scheint in der Praxis jedenfalls bislang noch keine nennenswerte Rolle zu spielen. Es ist jedoch nicht davon auszugehen, dass sich dies in Zukunft ändern wird. Die zeitlich begrenzte Zwischenspeicherung von Dateien macht den Cache-Provider wenig attraktiv für Rechteinhaber. Vielmehr werden diese sich auf die Ursprungsseite konzentrieren, auf welcher das Material originär gespeichert ist. Der Cache-Provider scheint nicht in deren Fokus zu liegen.

[1459] Field v. Google Inc., 412 F.Supp.2d 1106, 1124 (2006).
[1460] Field v. Google Inc., 412 F.Supp.2d 1106, 1124 (2006).
[1461] Nimmer on Copyright, § 12B.03 [A] [2]; Peguera, 56 J. Copyright Soc'y U.S.A. 589, 618 ff. (2009).
[1462] Peguera, 56 J. Copyright Soc'y U.S.A. 589, 621 (2009).
[1463] Nimmer on Copyright, § 12B.03 [A] [2].

d) Access-Provider

An erster Stelle gesetzlich in § 512 (a) DMCA geregelt ist die Privilegierung des Access-Providers.

Diesen trifft grundsätzlich keine Verantwortlichkeit für *„transmitting, routing, or providing connections for, material through a system or network controlled or operated by or for the service provider, or by reason of the intermediate or transient storage of that material in the course of transmitting, routing, or providing connections"*, sofern er die Voraussetzungen des § 512 (a) (1) – (5) DMCA erfüllt. Hintergrund der recht umfangreichen Haftungsfreistellung der Access-Provider ist deren gewichtige Rolle für das Funktionieren des Internet.

Teilweise wird die Auffassung vertreten, dass § 512 (a) DMCA die gesetzliche Verkörperung der „Netcom"-Entscheidung[1464] darstellt.[1465]

Hier wurde der Access-Provider, der den Zugang zum Usenet herstellte, als nicht verantwortlich für eine direkte Urheberrechtsverletzung (*direct infringement)* befunden.[1466] Die Frage der Verantwortlichkeit nach *secondary liability* wurde offen gelassen.

Eine solche Leseart ist allerdings deplatziert.[1467] Die *safe harbor*-Bestimmungen verändern nicht die allgemeinen Haftungsregelungen, sondern sie schränken vielmehr die Rechtsfolgen im Falle einer Haftung nach den allgemeinen Grundsätzen ein.[1468] Entsprechend wurde durch § 512 (a) DMCA

[1464] Religious Technology Center v. Netcom On-line Communication Services Inc., 907 F.Supp. 1361 (N.D.Cal. 1995).

[1465] Ellison v. Robertson, 357 F.3d 1072, 1081 (9th Cir. 2004); Ludwig, Boston College Intellectual Property & Technology Forum, 5 (2006); so auch noch im H. Rep. 105-551(I) zum alten Gesetzesentwurf des DMCA, S. 24: *„This exemption codifies the result of Religious Technology Center v. Netcom On-line Communications Services Inc., 907 F.Supp. 1361 (N.D. Cal. 1995) ('Netcom'), with respect to liability of providers for direct infringement.*"

[1466] Religious Technology Center v. Netcom On-line Communication Services Inc., 907 F.Supp. 1361, 1372 (N.D.Cal. 1995).

[1467] So auch Lovejoy, 27 Harv. J.L. & Tech. 257, 265 (2013).

[1468] Siehe S. Rep. 105-190, S. 19 *„Rather than embarking upon a wholesale clarification of these doctrines, the Committee decided to leave current law in its evolving state and, instead, to create a series of 'safe harbors', for certain common activities of service providers.".*

zwar eine ähnliche Herangehensweise mit teils gleichartigem Ergebnis gewählt, von einer Kodifizierung der tragenden Entscheidungsgründe kann allerdings keine Rede sein.

Für die Inanspruchnahme des *safe harbor* nach § 512 (a) DMCA ist es nicht erforderlich, dass das Material an sich rechtsverletzend ist.[1469] Die Immunität bezieht sich auf jegliches Material, nicht nur auf solches, welches unmittelbar Urheberrechte verletzt.[1470]

aa) Voraussetzungen

Um die Privilegierung des § 512 (a) DMCA in Anspruch nehmen zu können, muss der Access-Provider kumulativ die folgenden Voraussetzungen erfüllen.

(1) Vom Nutzer initiierte Übertragung

Gem. § 512 (a) (1) DMCA muss die Durchleitung des Materials entweder direkt von einer dritten Person oder auf Anweisung dieser initiiert worden sein (*transmission initiated by or at the direction of the user*). Durch diese Bestimmung soll sichergestellt werden, dass der *safe harbor* nicht für Übermittlungen gewährt wird, welche auf Willen des Access-Providers veranlasst werden.[1471]

(2) Keine Auswahl des Materials

Gem. § 512 (a) (2) DMCA muss es sich zudem um einen automatischen technischen Vorgang ohne jegliche Auswahl des Materials durch den Access-Provider handeln (*automatic technical process without selection of the material*). Der *House* und *Senate Report* stellen klar, dass es sich bei der Bezeichnung *selection of the material* um eine redaktionelle Auswahl des Materials, welches gesendet werden soll, handelt, im Gegenteil zu dem automatischen Prozess des Antwortens auf Befehle oder Anfragen eines Nutzers.[1472]

[1469] Perfect 10, Inc. v. CCBill LLC, 488 F.3d 1102, 1116 (9th Cir. 2007); Columbia Pictures Industries, Inc. v. Gary Fung, 710 F.3d 1020, 1041 (9th Cir. 2013).
[1470] Perfect 10, Inc. v. CCBill LLC, 488 F.3d 1102, 1116 (9th Cir. 2007).
[1471] Lovejoy, 27 Harv. J.L. & Tech. 257, 261 (2013).
[1472] H.R. Rep. 105-551(II), S. 51; S. Rep. 105-190, S. 42.

(3) Keine Auswahl der Empfänger

Als weitere Voraussetzung darf der Access-Provider gem. § 512 (a) (3) DMCA die Empfänger des Materials nicht ausgewählt haben (*no selection of the recipients of the material*). Der Empfänger muss vielmehr durch die automatische Beantwortung einer Nutzeranfrage ausgewählt werden.

Hierdurch wird nochmals der Ausschluss von redaktionellem oder willentlichem Verhalten des Access-Providers unterstrichen.[1473] Lediglich automatische Rückmeldungen auf Nutzeranfragen werden erfasst.[1474]

(4) Keine dauerhafte Kopie

Der Access-Provider darf weiterhin gem. § 512 (a) (4) DMCA keine Kopie des Materials in einer Weise auf seinem System oder in seinem Netzwerk speichern, die es dritten Personen erlaubt auf diese zuzugreifen sowie keine Kopie für einen Zeitraum länger als notwendig zur Durchleitung, Weiterleitung oder Bereitstellung einer Verbindung speichern (*no copy of the material is maintained in a manner ordinarily accessible to anyone or for a time longer then reasonably neccessary*).

Der Begriff *ordinarily accessible* soll klarstellen, dass hiervon nicht Eindringlinge erfasst werden, die sich illegal Zugang zu dem Material verschaffen.[1475] Hierzu zählen allerdings solche Kopien, die der ISP zu dem Zwecke macht, diese anderen Nutzer zugänglich zu machen. In diesem Fall handelt es sich um einen Cache-Provider und somit ist § 512 (b) DMCA einschlägig. Auch wird durch dieses Merkmal der Access-Provider vom Host-Provider abgegrenzt, welcher Inhalte zur allgemeinen Verfügbarkeit speichert.[1476]

Für welchen Zeitraum eine entsprechende Speicherung notwendig ist, wurde gesetzlich nicht festgeschrieben. In *Ellison v. Robertson* hat der *Ninth Circuit* entschieden, dass sich ein Access-Provider,

[1473] Lovejoy, 27 Harv. J.L. & Tech. 257, 261 (2013).
[1474] H.R. Rep. 105-551(II), S. 51; S. Rep. 105-190, S. 42.
[1475] H.R. Rep. 105-551(II), S. 51; S. Rep. 105-190, S. 42.
[1476] Lovejoy, 27 Harv. J.L. & Tech. 257, 261 (2013).

der das streitgegenständliche Urheberrechtsmaterial für eine Dauer von 14 Tagen speichert, für den Schutz des § 512 (a) DMCA qualifiziert.[1477] Das Gericht hat sich hier an dem frühen „Netcom"-Fall, welcher vor Einführung der Haftungsprivilegien entschieden wurde, orientiert.[1478] In diesem ging es um die Haftung eines Access-Providers, welcher den Zugang zum Usenet vermittelte und in diesem Zusammenhang das streitgegenständliche Material für eine Dauer von 11 Tagen zwischenspeicherte. Das Gericht befand den Access-Provider hier für nicht *direct liable*, da dieser lediglich ein System unterhielt, in dem die Nachrichten der Nutzer durch Software automatisch weitergeleitet und im Zuge dessen temporär gespeichert wurden.[1479]

(5) Keine Veränderung des Inhalts

Letztendlich darf der Access-Provider gem. § 512 (a) (5) DMCA das übermittelte Material inhaltlich nicht ändern (*transmission without modification of the content*). Wichtig ist, dass hier lediglich der Inhalt durch den Access-Provider nicht verändert werden darf. Änderungen der Form können grundsätzlich erlaubt sein, beispielsweise Änderungen der Formatierung während der Übertragung einer E-Mail.[1480]

bb) Anwendbarkeit auf WLAN-Betreiber

Fraglich ist, ob § 512 (a) DMCA auch für private oder kommerzielle Anbieter von öffentlichen WLAN-Netzen Anwendung findet. Die Literatur hierzu ist bislang dürftig, auch Rechtsprechung ist nicht bekannt.

Es ist jedoch kein Grund ersichtlich, warum der Anbieter eines offenen WLAN nicht in den Genuß der Haftungsprivilegierung kommen sollte, sofern er alle Voraussetzungen erfüllt.[1481]

[1477] Ellison v. Robertson, 357 F.3d. 1072, 1081 (9th Cir. 2004).
[1478] Religious Technology Center v. Netcom On-line Communication Services Inc., 907 F.Supp. 1361 (N.D.Cal. 1995).
[1479] Religious Technology Center v. Netcom On-line Communication Services Inc., 907 F.Supp. 1361, 1372 (N.D.Cal. 1995).
[1480] H.R. Rep. 105-551(II), S. 51; S. Rep. 105-190, S. 19.
[1481] So auch Watkins, Wireless Liability, S. 25 f. (2013); Scott on Multimedia Law, § 4.37 [B] [1].

Allerdings ist zu beachten, dass nicht nur die fünf Voraussetzungen des § 512 (a) DMCA zu erfüllen sind, sondern auch die allgemeinen Voraussetzungen. Problematisch könnte hier insbesondere das Erfordernis der Implementierung einer *repeat infringer policy* sein. Während kommerzielle Betreiber, wie bspw. Coffee Shops, eine solche noch in ihren AGB einbinden können, ist eine entsprechende Einbindung durch private Personen, die ihren Anschluss nicht mit einem Passwort versehen und damit Dritten zur Verfügung stellen, eher abwegig. Allerdings könnte man in diesen Fällen argumentieren, dass keine Verpflichtung zur Implementierung einer derartigen *policy* besteht, da der private WLAN-Anschlussinhaber weder über Abonnenten noch Kontoinhaber verfügt.[1482] Im Übrigen kann dies auch bei gewerblichen WLAN-Betreibern der Fall sein, sofern die Nutzung des Netzwerkes keine vorherige Registrierung erfordert.

Zudem wird teilweise angebracht, dass aufgrund des Wortlauts *„entity"*[1483], individuelle Einzelpersonen von dem *safe harbour* des § 512 (a) DMCA grundsätzlich ausgeschlossen sind.[1484] Eine entsprechende Eingrenzung des Anwendungsbereichs auf *entities* findet sich nicht für die anderen ISP in § 512 (k) (1) (B) DMCA wieder, dort wird der Begriff des *providers* bzw. *operators* verwendet.[1485] Es ist unklar, warum der Gesetzgeber hier eine scheinbare Unterscheidung vornimmt. Auch die Gesetzgebungsmaterialien schweigen hierzu. Es ist allerdings schwer herzuleiten, warum im Bereich der Zugangsvermittlung die Privilegierung lediglich Unternehmen erfassen sollte während im Bereich des Hosting oder des Caching auch Einzelpersonen erfasst

[1482] Siehe hinsichtlich der diesbezüglichen Diskussion S. 261.
[1483] § 512 (k) (1) (A) DMCA: *„[...] the term 'service provider' means an entity offering the transmission, routing, or providing of connections for digital online communications [...]"*.
[1484] Ballon, E-Commerce & Internet Law (2014-2015 Update), 4.12[2].
[1485] § 512 (k) (1) (B) DMCA: *„[...] the term „service provider" means a provider of online services or network access, ort he operator of facilities therefor [...]"*.

werden. Daher ist nach der hier vertretenen Auffassung § 512 (a) DMCA gleichwohl auch auf Einzelpersonen anzuwenden.[1486]

cc) Fazit

Da der Access-Provider in der Regel lediglich die technische Infrastruktur zur Übertragung von Inhalten bereitstellt, hat er durch den DMCA die umfangreichste Privilegierung erfahren. Vollkommen irrelevant ist eine etwaige Kenntnis des Access-Providers. Anders als der Host-Provider ist die Privilegierung des Access-Providers nicht abhängig von der Kenntnis über urheberrechtsverletzendes Material und entsprechend würden auch Monitoringmaßnahmen seitens des Access-Providers zu keinem Verlust der Haftungsprivilegierung führen.[1487]

In der Praxis spielt § 512 (a) DMCA daher bislang eine lediglich untergeordnete Rolle. In der öffentlichen Debatte geht es vielmehr um die Rolle der ISP im Kampf der Inhalteindustrie gegen Peer-to-Peer Filesharer. Von Bedeutung sind in diesem Zusammenhang privatrechtliche Vereinbarungen zwischen Access-Providern und ISP sowie die Möglichkeit der Identifizierung potentieller Rechtsverletzer durch die Access-Provider.

e) Information Location Tools

Gem. § 512 (d) DMCA ist der Provider nicht verantwortlich für Urheberrechtsverletzungen aufgrund des Verweisens oder Verlinkens von Nutzern zu einer *„online location containing infringing material or infringing activity, by using information location tools, including a directory, index, reference, pointer, or hypertext link"*. Der Privilegierung der *Information Location Tools* liegt der Gedanke zugrunde, dass diese essentiell für den Betrieb des Internet sind und der Nutzer ohne sie die Informationen, die er benötigt, nicht bzw. nur schwer auffinden könnte.[1488] Der *House* und *Senate Report* heben in diesem Zusammenhang besonders die

[1486] So auch Stoltz, Victory for Open WiFi: Judge Rejects Copyright Troll's Bogus „Negligence" Theory.
[1487] Ballon, E-Commerce & Internet Law (2014-2015 Update), 4.12[4].
[1488] H.R. Rep. 105-551(II), S. 58; S. Rep. 105-190, S. 49.

Bedeutung der Webverzeichnisse (*directories*), wie das von Yahoo!, hervor.[1489] Webverzeichnisse sind Sammlungen von Webseiten, die nach bestimmten Kategorien und Themen organisiert sind. Im Unterschied zu der Tätigkeit von Suchmaschinen wie Google werden die Suchergebnisse nicht anhand von Keywords angezeigt, sondern der Nutzer selbst klickt sich durch die Kategorien und Unterkategorien, um so zu dem gesuchten Inhalt zu gelangen. Die Verzeichnisse werden nicht durch *web crawler*, sondern durch die Webverzeichnis-Redaktion erstellt. Diese durchsuchen das Internet, sichten und sammeln Informationen und kategorisieren diese in ihrem Verzeichnis. Der *safe harbor* für *Information Location Tools* wurde eingeführt, um die Entwicklung dieser Webverzeichnisse zu fördern.[1490] Heutzutage sind die Webverzeichnisse jedoch kaum noch von Bedeutung, das Yahoo! Webverzeichnis wurde in vielen europäischen Ländern, u.a. Deutschland, bereits 2009 einstellt[1491], 2014 folgte die komplette Einstellung des Dienstes.[1492] Sie wurden durch Suchmaschinen, wie Google, die das Internet automatisch durch *web crawler* durchsuchen, ersetzt. Im Gegensatz zum Webverzeichnis findet keine menschliche Interaktion mehr statt.
Die Voraussetzungen, um in den Genuss der Haftungsprivilegierung zu gelangen, sind parallel zu denen, die der Host-Provider zu erfüllen hat.

aa) Keine tatsächliche Kenntnis – No actual knowledge

Der Provider darf gem. § 512 (d) (1) (A) DMCA zunächst keine Kenntnis von dem rechtsverletzenden Material oder der rechtsverletzenden Tätigkeit haben. Da bislang kaum Rechtsprechung hinsichtlich § 512 (d) DMCA ergangen ist und auch die Gesetzgebungsmaterialien lediglich auf den *safe harbor* des Host-Providers unter § 512 (c) DMCA verweisen, kann bzgl.

[1489] H.R. Rep. 105-551(II), S. 58; S. Rep. 105-190, S. 49.
[1490] H.R. Rep. 105-551(II), S. 58; S. Rep. 105-190, S. 49.
[1491] Siehe McGee, Yahoo Closes European Directories.
[1492] Siehe Sullivan, The Yahoo Directory Is To Close.

des Merkmals der actual knowledge auf die diesbezüglichen Ausführungen unter D.III.5.b)cc)(1) verwiesen werden.

bb) No awareness – Keine red flag knowledge

Gem. § 512 (d) (1) (B) DMCA darf sich der Provider auch keiner Tatsachen oder Umstände bewusst sein, aus denen eine rechtsverletzende Handlung offensichtlich ist. Der *House* und *Senate Report* führen diesbezüglich beispielhaft aus, dass der Urheberrechtsinhaber eine solche *awareness* des Providers aufzeigen könne, indem er nachweist, dass die verlinkte Seite, zu dem Zeitpunkt als der Provider des Webverzeichnisses sie betrachtete, eindeutig eine Piraterie-Webseite darstellte, auf der Tonaufnahmen, Software, Filme oder Bücher für unautorisiertes Herunterladen oder zur öffentlichen Wiedergabe zur Verfügung standen.[1493] Auf der anderen Seite läge eine entsprechende *awareness* des Providers nicht bereits deshalb vor, weil er ein oder mehrere bekannte Fotografien eines Prominenten auf einer Seite sieht, welche diesem gewidmet ist.[1494] Es könne von dem Provider nicht verlangt werden, während seines kurzen Besuchs auf der Webseite zu Katalogisierungszwecken, zu bestimmten, ob die Fotografie noch urheberrechtlich geschützt ist oder es sich bereits um Gemeingut handelt, ob die Nutzung lizenziert ist oder ob sie unter der *Fair Use*-Doktrin[1495] erlaubt ist.[1496]

Ziel dieser Regelung sei es, ausgefeilte Piraterie-Webverzeichnisse, welche den Nutzer zu anderen ausgewählten Webseiten verlinken, auf denen Piraterie-Software, -Bücher, -Filme- oder -Musik heruntergeladen werden können, von dem Schutz des *safe harbor* auszuschließen.[1497] Solche Webverzeichnisse verwiesen Nutzer auf Webseiten, die offensichtlich rechtsverletzend seien, da sie typischerweise Begriffe wie „pirate“, „bootleg“ oder andere umgangssprachliche Ausdrücke in ihrer URL verwenden, die den

[1493] H.R. Rep. 105-551(II), S. 57; S. Rep. 105-190, S. 48.
[1494] H.R. Rep. 105-551(II), S. 57; S. Rep. 105-190, S. 48.
[1495] *Fair use* ist die Schrankenbestimmung des US-amerikanischen Urheberrechts, siehe 17 U.S.C. § 107.
[1496] H.R. Rep. 105-551(II), S. 58; S. Rep. 105-190, S. 48.
[1497] H.R. Rep. 105-551(II), S. 58; S. Rep. 105-190, S. 48.

illegalen Zweck offenbarten.[1498] Da die rechtsverletzende Natur dieser Webseiten sich auch nur aufgrund eines flüchtigen Blickes offenbaren würde, wäre eine Privilegierung des Providers, der eine solche Seite besucht und diese anschließend verlinkt, nicht angemessen.[1499] Es sei daher in einem solchen Fall gerechtfertigt, durch die Beweisführung des Urheberrechtsinhabers, dass der Provider eine entsprechende Seite besucht hat, dessen Anspruch auf *safe harbor* zu widerlegen.[1500]

Als Ergebnis würde eine gerechte Balance hergestellt werden, indem die Redakteure des Providers grundsätzlich nicht dazu verpflichtet seien differenzierte Beurteilungen vorzunehmen, lediglich eine offensichtliche Piraterie-Webseite im vorgenannten Sinne würde eine *red flag* konstituieren.[1501]

Da Webverzeichnisse mit redaktioneller Auswahl der Webseiten heutzutage kaum noch angeboten werden, kommt auch der Gesetzesbegründung zur *red flag knowledge* nur noch eine geringe Bedeutung zu. Eine Übertragbarkeit der Ausführungen auf Suchmaschinen ist fraglich.[1502] Diese setzen *web crawler* ein, welche das Netz vollkommen autonom und ohne jegliche menschliche Interaktion durchsuchen und bei einer Suchanfrage des Nutzers mit den Ergebnissen dieser Suche beliefern. Der Suchmaschinen-Anbieter hat in der Regel keine genaue Kenntnis über die von dem *web crawler* durchsuchten Webseiten. Entsprechend ist auch für ihn nicht offensichtlich, ob es sich um eine Piraterie-Webseite handelt.[1503]

Information Location Tools trifft jedenfalls keine Pflicht, Urheberrechtsverletzungen in ihrem System ausfindig zu machen, sofern sie allerdings die Augen vor *red flags*, also offensichtlichen

[1498] H.R. Rep. 105-551(II), S. 58; S. Rep. 105-190, S. 48.
[1499] H.R. Rep. 105-551(II), S. 58; S. Rep. 105-190, S. 48.
[1500] H.R. Rep. 105-551(II), S. 58; S. Rep. 105-190, S. 48 f.
[1501] H.R. Rep. 105-551(II), S. 58; S. Rep. 105-190, S. 49.
[1502] So auch Blom, 1 Case W. Reserve J.L. Tech. & Internet 36, 49 (2009).
[1503] Hinsichtlich der Offensichtlichkeit einer Webseite mit rechtswidrigen Inhalten augrund der Beschreibung mit Begriffen wie „pirate“ oder „bootleg“ kann auf die Begründung des *Ninth Circuit* in Perfect 10, Inc. v. CCBill LLC, 488 F.3d 1102, 1114 (9th Cir. 2007) verwiesen werden, siehe S. 272.

Rechtsverletzungen verschließen, verlieren auch sie auch ihren *safe harbor*.[1504]

cc) Entfernung bzw. Sperrung des Materials

Hat der Provider *actual knowledge* oder *awareness* von dem rechtswidrigen Material, hat er dies gem. § 512 (d) (1) (C) DMCA zu entfernen bzw. den Zugang hierzu zu sperren. Gemeint ist hiermit nicht, wie in § 512 (c) (1) (A) (iii) DMCA, das rechtswidrige Material an sich, sondern der Verweis/Link hierauf. Bezüglich der weiteren Voraussetzungen kann auf D.III.5.b)cc)(4) verwiesen werden.

dd) Finanzieller Vorteil und Kontrolle

Entsprechend § 512 (c) (1) (B) DMCA, darf der Provider gem. § 512 (d) (2) DMCA keinen direkten finanziellen Vorteil aus der Rechtsverletzung ziehen, sofern er das Recht und die Möglichkeit der Kontrolle über diese hatte. Da es diesbezüglich keine anderweitigen gesetzgeberischen oder gerichtlichen Ausführungen gibt, kann hinsichtlich der allgemeinen Voraussetzungen auf die gleichlautende Bestimmung des Host-Providers verwiesen werden.[1505]

ee) Notice and Takedown-Verfahren

§ 512 (d) (3) DMCA bestimmt, dass der Provider nach Erhalt einer *notification* gem. § 512 (c) (3) DMCA das Material zu entfernen bzw. den Zugang hierzu zu sperren hat. Zur Klarstellung wird ausgeführt, dass die Information gem. § 512 (c) (3) (A) (iii) DMCA im Falle der *Information Location Tools* die Identifizierung des Verweises/Links, der auf die Rechtsverletzung verweist und der entsprechend zu entfernen bzw. zu blockieren ist, betrifft und Informationen, die es dem Provider ermöglichen, diesen Verweis/Link aufzufinden.

Für die weiteren Voraussetzungen kann entsprechend auf D.III.5.b)ee)(2) verwiesen werden.

[1504] H.R. Rep. 105-551(II), S. 57; S. Rep. 105-190, S. 48.
[1505] Siehe hierzu S. 287.

Es existiert bislang nur wenig Rechtsprechung in dieser Hinsicht. In *Arista Records v. MP3 Board* hat der *S.D.N.Y.* ausgeführt, dass eine *notification*, welche zwar keine spezifischen URLs der behaupteten Rechtsverletzungen enthalte unschädlich sei, da sowohl die Künstler und Songs aufgelistet waren als auch Ausdrucke von Screenshots beigefügt wurden, in welchen die relevanten Links hervorgehoben und entsprechend markiert wurden.[1506] Das Gericht verwarf damit das Argument von MP3Board, dass die *notification* nicht den Anforderungen des DMCA entsprechen würde, da die Links nicht in elektronischer Form übermittelt wurden und nicht die einzelnen URLs auf welche die Links verwiesen, angegeben worden seien.[1507] Aufgrund der Screenshots mit den Links auf der Webseite von MP3Board sei das Material, welches als urheberrechtswidrig beanstandet werde, ausreichend kenntlich gemacht, so dass MP3Board in die Lage versetzt werde, die Links zu lokalisieren.[1508]

Nicht notwendig ist zudem eine Benachrichtigung nach § 512 (g) (2) (A) DMCA. Da der Provider eines *Information Location Tools* i.d.R. in keiner vertraglichen Beziehung zu dem behaupteten Rechtsverletzer steht, wird er oftmals auch nicht die Möglichkeit haben, eine entsprechende Benachrichtigung zu erteilen.[1509] Zudem spricht § 512 (g) (2) (A) DMCA lediglich von der Benachrichtigung des *subscribers*.

ff) Allgemeine und spezialisierte Suchmaschinen

In den letzten Jahren tauchen neben den allgemeinen Suchmaschinen (*generalized search engines*) wie Google, vermehrt spezialisierte Suchmaschinen (*specialized search engines*) auf, in welchen explizit nach Musikdateien gesucht werden kann.[1510] Der Nutzer gibt wie bei der allgemeinen Suchmaschine den Namen der

[1506] Arista Records, Inc. v. MP3Board, Inc., 00 Civ. 4660 (SHS), 2002 U.S. Dist. LEXIS 16165 at *29 (S.D.N.Y. Aug. 28, 2002).
[1507] Arista Records, Inc. v. MP3Board, Inc., 00 Civ. 4660 (SHS), 2002 U.S. Dist. LEXIS 16165 at *30 (S.D.N.Y. Aug. 28, 2002).
[1508] Arista Records, Inc. v. MP3Board, Inc., 00 Civ. 4660 (SHS), 2002 U.S. Dist. LEXIS 16165 at *30 (S.D.N.Y. Aug. 28, 2002).
[1509] Urban/Quilter, 22 Santa Clara Computer & High Tech. L.J. 621, 626 (2006).
[1510] Civilini, 19 UCLA Ent. L. Rev. 407, 411 (2012).

gesuchten Musikdatei ein und ihm wird eine Liste von Links angezeigt.[1511] Will der Nutzer sich eine dieser Dateien auf seinen Computer herunterladen, hat er lediglich den Link anzuklicken und der ausgewählte Song wird von der originalen Webseite heruntergeladen ohne dass der Nutzer diese Webseite besucht.[1512] Der Nutzer bleibt während des gesamten Ablaufs auf der Seite des Suchmaschinenanbieters.[1513]

Im Gegensatz zu allgemeinen Suchmaschinen, welche regelmäßig in den Anwendungsbereich des § 512 (d) DMCA fallen[1514], ist es fraglich, ob solche spezialisierten Suchmaschinen überhaupt den Schutz der *safe harbor*-Bestimmungen für *Information Location Tools* beanspruchen können. *Civilini* geht, ohne nähere Erläuterung, davon aus, dass spezialisierte Suchmaschinen nicht von dem *safe harbor* des DMCA erfasst werden.[1515] Dem ist so nicht zuzustimmen. Ob eine spezialisierte Suchmaschine in den Schutzbereich des DMCA *safe harbor* fällt, hängt von der konkreten Ausgestaltung des Services sowie den jeweiligen Umständen des Einzelfalls ab. Ein kategorischer Ausschluss ist nicht geboten. So hat der *S.D.N.Y.* beispielsweise Sideload.com, eine Internetsuchmaschine, die es Nutzern erlaubt, nach freien Musikdateien im Internet zu suchen, dem Schutz des DMCA *safe harbor* unterworfen.[1516] Sofern die spezialisierte Suchmaschine aufgrund der Umstände des Einzelfalls keinen Schutz des DMCA beanspruchen kann, wäre hier insbesondere eine Haftung im Wege der *inducement liability* denkbar, sofern der Suchmaschinenanbieter es darauf angelegt hat, Urheberrechtsverletzungen mit seinem Dienst Vorschub zu leisten.

[1511] Civilini, 19 UCLA Ent. L. Rev. 407, 411 (2012).
[1512] Civilini, 19 UCLA Ent. L. Rev. 407, 412 (2012).
[1513] Civilini, 19 UCLA Ent. L. Rev. 407, 412 (2012).
[1514] Civilini, 19 UCLA Ent. L. Rev. 407, 434 (2012).
[1515] Civilini, 19 UCLA Ent. L. Rev. 407, 438 (2012).
[1516] Capitol Records, Inc. v. MP3Tunes, LLC, 821 F.Supp.2d 627, 639 (S.D.N.Y. 2011).

gg) Fazit

Zur Anwendung der *safe harbor*-Bestimmungen auf *Information Location Tools* existiert bislang kaum Rechtsprechung. Dies liegt zum einen daran, dass Rechteinhaber aus Effizienzgründen meist entweder gegen den direkten Rechtsverletzer oder den Host-Provider vorgehen werden, der das rechtsverletzende Material auf seiner Plattform für den Nutzer speichert. Zum anderen liegt es insbesondere im Hinblick auf allgemeine Suchmaschinen daran, dass diese eine wichtige Rolle im Internet einnehmen und sowohl für Nutzer als auch für Rechteinhaber von großem Nutzen sind, da viele Nutzer erst durch die Suchmaschinen auf bestimmte Inhalte aufmerksam und zu diesen verlinkt werden.

Bislang ist kein Fall bekannt, in dem ein Rechtsinhaber eine allgemeine Suchmaschine wegen Urheberrechtsverletzungen verklagt hätte.[1517]

Anders verhält es sich jedoch mit spezialisierten Suchmaschinen. Hier haben Urheberrechtsinhaber bereits des Öfteren eine Haftung auf dem Klageweg angestrebt.[1518] Das Resultat dieser Bemühungen ist mehr oder weniger von Erfolg gekrönt. Während eine Haftung aufgrund von Urheberrechtsverletzungen in keinem der Fälle festgestellt wurde, führten die horrenden Kosten der gegen den Dienst SeeqPod geführten Klagen dazu, dass, ganz im Sinne der Rechtsinhaber, das Unternehmen in den Konkurs getrieben wurde.[1519]

Auch in *A&M Records v. Napster* erkannte der *Ninth Circuit* die grundsätzlich mögliche Anwendbarkeit des § 512 (d) DMCA zwar an, führte diesbezüglich aber nicht weiter aus und ließ die Frage somit unbeantwortet.[1520]

[1517] Civilini, 19 UCLA Ent. L. Rev. 407, 432 (2012).

[1518] Vgl. bspw. Warner Bros. Records, Inc. v. SeeqPod, Inc., No. 08 CV 00335 (C.D. Cal.), 2007 WL 4837988; Capitol Records, L.L.C. v. SeeqPod, Inc., No. 09 Civ. 1584 (S.D.N.Y. 2010), 2010 WL 481228; Capitol Records, Inc. v. MP3Tunes, LLC, 821 F.Supp.2d 627 (S.D.N.Y. 2011).

[1519] Civilini, 19 UCLA Ent. L. Rev. 407, 440 (2012).

[1520] A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1025; *„We do not agree that Napster's potential liability for contributory and vicarious infringement renders the Digital Millennium Copyright Act inapplicable per se. We instead recognize that this issue will be more fully developed at trial."*

Hauptkritikpunkt an den gesetzlichen *safe harbor* Bestimmungen des DMCA für *Information Location Tools* ist die praktisch fehlende Möglichkeit des Nutzers gegen gelöschte Suchergebnisse vorzugehen.[1521] Denn anders als bei dem Host-Provider sieht das gesetzliche Konstrukt keine Benachrichtigung des Nutzers über die Entfernung eines Links, keine *counter notification* sowie kein *put back*-Verfahren vor. Zwar ist bei der Entfernung eines Links das Material noch an seinem Ursprungsort auffindbar, allerdings ist ein Auffinden dieser Inhalte ohne entsprechende Auflistung in den Ergebnislisten der Suchmaschine oftmals nahezu unmöglich. Auch führe die fehlende vertragliche Beziehung zu den Nutzern der *Information Location Tools* dazu, dass diese noch anfälliger als der Host-Provider dafür sind, als urheberrechtsverletzend geltend gemachtes Material übereifrig zu entfernen.[1522]

f) Counter notification

Da das *Notice and Takedown*-Verfahren dem ISP bereits die Kenntnis einer Rechtsverletzung zuschreibt, sofern lediglich die formalen Anforderungen an die *notification* erfüllt sind, enthält § 512 (g) (2) DMCA das sog. *counter notification*-Verfahren, dass dem behaupteten Rechtsverletzer die Möglichkeit einräumt sich durch das Verfassen einer *counter notification* gegen die behauptete Rechtsverletzung zu wehren.

aa) Voraussetzungen der counter notification

Ist der *subscriber* der Auffassung, dass das Material zu Unrecht entfernt bzw. blockiert wurde, so kann er den ISP anhand einer *counter notification* gemäß § 512 (g) (3) DMCA hierüber in Kenntnis setzen.

Die *counter notification* ist von dem *subscriber* handschriftlich bzw. elektronisch zu unterzeichnen.[1523] Sie muss zudem das Material bezeichnen, welches gelöscht bzw. blockiert wurde und

[1521] So z.B. Urban/Quilter, 22 Santa Clara Computer & High Tech. L.J. 621, 690 (2006).
[1522] Blom, 1 Case W. Reserve J.L. Tech. & Internet 36, 54 (2009).
[1523] § 512 (g) (3) (A) DMCA; vgl. bzgl. dem Erfordernis der elektronischen Unterschrift siehe S. 301.

die Stelle benennen, wo das Material vor Löschung bzw. Sperrung enthalten war.[1524] Weiterhin muss der *counter notification* eine eidesstattliche Erklärung beigefügt werden, dass der *subscriber* in gutem Glauben davon ausgeht, dass das Material aufgrund eines Fehlers bzw. einer falschen Identifizierung gelöscht bzw. gesperrt wurde.[1525]

Sowohl Rechteinhaber als auch vermeintlicher Rechtsverletzer haben hinsichtlich der innerhalb der *notification* bzw. *counter notification* gemachten Angaben zu versichern, dass sie in gutem Glauben handeln. Unklar ist allerdings, warum der vermeintliche Rechtsverletzer insoweit strengeren Maßgaben unterliegt als der ursprüngliche Absender der *notification*. Denn während der Absender der *notification* lediglich eidesstattlich zu versichern hat, dass er vom Urheberrechtsinhaber autorisiert wurde, für diesen zu handeln, hat der Absender der *counter notification* seinen guten Glauben hinsichtlich der unberechtigten Entfernung seines Materials eidesstattlich zu versichern.[1526]

Zudem hat der *subscriber* seinen Namen, seine Adresse und Telefonnummer anzugeben sowie eine Erklärung, dass er sich mit der Zuständigkeit des *Federal District Court* des Gerichtsbezirks seines Wohnsitzes einverstanden erklärt, und falls dieser außerhalb der USA liegt, mit der Zuständigkeit des Gerichtsbezirks des ISP und dass er die Klagezustellung von derjenigen Person, die zuvor die *notification* unter § 512 (c) (1) (C) DMCA eingereicht hat bzw. deren Bevollmächtigten, akzeptiert.[1527]

Die *counter notification* muss im Wesentlichen mit diesen Anforderungen übereinstimmen, bzgl. des Standards einer

[1524] § 512 (g) (3) (B) DMCA.
[1525] § 512 (g) (3) (C) DMCA.
[1526] So auch Ballon, 4.12[9][D], der die Möglichkeit in Betracht zieht, dass diese Unstimmigkeit auf einem Fehler bei der Abfassung des § 512 (c) (3) (A) (vi) DMCA beruht und nicht lediglich die Autorisierung der Beschwerde führenden Partei eidesstattlich versichert werden soll, sondern auch die Richtigkeit der in der *notification* gemachten Angaben allgemein.
[1527] § 512 (g) (3) (D) DMCA.

wesentlichen Übereinstimmung kann auf D.III.5.b)ee)(2) verwiesen werden.[1528]

Das Gesetz schreibt keine zeitliche Frist für die Einreichung einer *counter notification* vor.

Wie auch bei der *notification* muss das für die *counter notification* implementierte System des ISP mit den gesetzlichen Vorgaben übereinstimmen.[1529] Der *N.D. California* hat entsprechend ausgeführt, dass ein *counter notification*-Prozedere, welches keine Erklärung erfordert, dass der *subscriber* im guten Glauben davon ausgeht, dass das Material aufgrund eines Fehlers bzw. einer falschen Identifizierung gelöscht bzw. gesperrt wurde, die gesetzlichen Voraussetzungen verwässere und das sorgfältig austarierte System des DMCA aus dem Gleichgewicht bringe.[1530]

Entsprechend kann eine Nichtbeachtung der gesetzlichen Vorgaben zum *counter notification* Prozedere die Privilegierung des ISP wegfallen lassen.

bb) Anwendungsbereich

Fraglich ist, für welche der im DMCA aufgeführten ISP diese Bestimmung Anwendung findet. Da die *counter notification* in einem separaten Absatz des § 512, unabhängig von denen der vier ISP, könnte man davon ausgehen, dass dieser gleichermaßen für alle ISP gilt, jedenfalls für diejenigen Provider, die sich auf das *Notice und Takedown*-Verfahren berufen können.

Nach dem Wortlaut des § 512 (g) (2) DMCA gilt die *counter notification* und damit auch das damit einhergehende *put back procedure*[1531] allerdings nur für Host-Provider.[1532] Nur der Host-Provider wird zudem i.d.R. über *subscriber* verfügen. Sowohl *Information Location Tools* als auch der Cache-Provider stehen im

[1528] H.R. Rep. 105-551(II), S.60; S. Rep. 105-190, S. 51.
[1529] Zur *notification* siehe diesbezüglich S. 310.
[1530] Perfect 10, Inc. v. Cybernet Ventures, Inc., 213 F.Supp.2d 1146, 1180 (2002).
[1531] Siehe hierzu S. 336.
[1532] *„[...] with respect to material residing at the direction of a subscriber [...]“;* siehe auch Walker, Virginia Journal of Law & Technology, Vol. 9, No. 2, para. 43, welcher jedenfalls auch das *counter notification procedure* für *search engines* als unanwendbar erklärt aufgrund der Nutzung des Begriffs der *subscriber*.

Regelfall in keiner vertraglichen Beziehung zu dem Nutzer ihrer Dienste.

Als Rechtfertigung für diese Ungleichbehandlung könnte die Tatsache sprechen, dass sowohl bei der Entfernung des Materials durch den Cache-Provider sowie die *Information Location Tools*, das gelöschte Material nicht die Ursprungsseite auf dem das Material vorhanden ist, betrifft. Es wird lediglich die Verlinkung zu dieser Ursprungsseite bzw. die Zwischenspeicherung des Materials von dieser Ursprungsseite gelöscht, nicht jedoch das Material selbst. Insbesondere hinsichtlich des *Information Location Tools* ist eine Löschung von Links ohne Unterrichtung des Inhalteanbieters sowie ohne die Möglichkeit zur Einreichung einer *counter notification* allerdings besonders heikel.

g) Put back procedure

Erhält der ISP eine *counter notification* entsprechend § 512 (g) (3) DMCA, so ist er gehalten, dem Absender der *notification* nach § 512 (c) (1) (C) DMCA umgehend eine Kopie der *counter notification* zukommen zu lassen und ihn darüber zu informieren, dass er das entfernte Material ersetzen bzw. die Sperrung des Materials innerhalb von 10 Werktagen aufheben wird.[1533] Zudem hat er das Material nicht früher als 10 Tage und nicht später als 14 Tage nach Erhalt der *counter notification* zu ersetzen bzw. die Sperrung aufzuheben, es sei denn sein Bevollmächtigter erhält zuvor eine Benachrichtigung darüber, dass der Absender der *notification* gegen den Nutzer eine Unterlassungsklage eingereicht hat.[1534] Da die Frist mit Erhalt der *counter notification* durch den ISP beginnt, kann sich auch eine verspätete Mitteilung des ISP an den Rechteinhaber auswirken, da dieser innerhalb dieser Frist eine Klage einreichen muss, um die Wiederherstellung des Inhaltes zu verhindern.[1535]

[1533] § 512 (g) (2) (B) DMCA.
[1534] § 512 (g) (2) (C) DMCA.
[1535] Ballon, 4.12[9][C].

Folgt der ISP dem *put back procedure* kann er gem. § 512 (g) (4) DMCA nicht dafür verantwortlich gemacht werden, dass er das Material wieder zugänglich gemacht hat.

Dies bedeutet, dass auch im Falle einer *counter notification* das Material zunächst für mindestens 10 Tage offline ist. Dies ist insbesondere für zeitkritisches Material von Bedeutung, wie bspw. Materialien zu einer aktuellen politischen Kampagne. So wurde im Jahr 2008 ca. 3 Wochen vor den Präsidentschaftswahlen in den USA ein Kampagnenvideo von Präsidentschaftskandidat McCain aufgrund einer *notification* von YouTube entfernt. Da es sich bei der Nutzung von Ausschnitten aus News-Sendungen offensichtlich um einen Fall des *fair use* handelte, sendete das McCain Kampagnen-Team eine *counter notification*. Es monierte allerdings den langen Zeitraum bis zur Wiederfreigabe des entfernten Inhaltes, da insbesondere kurz vor den Wahlen jeder Tag zähle.[1536]

h) Haftung gegenüber dem Nutzer

Gem. § 512 (g) (1) DMCA trifft den ISP keine Verantwortlichkeit gegenüber einer anderen Person hinsichtlich der Entfernung oder Sperrung von Material aufgrund einer tatsächlichen Kenntnis oder einer *red flag*, sofern er hierbei in gutem Glauben gehandelt hat.[1537] Dies gilt unabhängig davon, ob letzten Endes festgestellt wird, dass das Material tatsächlich rechtsverletzend ist. Hierdurch soll der ISP, der lediglich in gutem Glauben den gesetzlichen Bestimmungen des § 512 (c) DMCA folgt, von der Haftung freigestellt werden.[1538]

Aus dem Wortlaut dieser Vorschrift sowie den Gesetzgebungsmaterialien ergibt sich, dass diese Bestimmung lediglich auf den Cache- und Host-Provider sowie die *Information Location Tools* anwendbar ist.[1539] Da den Access-Provider keine

[1536] Rangnath, The McCain Campaign's Run In With The DMCA Highlights Need For More Balanced Copyright Law.

[1537] Auch „*Good Samaritan*"-Verteidigung genannt, siehe H.R. Rep. 105-551(I), S. 26.

[1538] H.R. Rep. 105-551(II), S. 59; S. Rep. 105-190, S. 50.

[1539] H.R. Rep. 105-551(II), S. 59: *„The purpose of this subsection is to protect service providers from liability to third parties whose material service providers*

entsprechende gesetzliche Pflicht zur Entfernung oder Sperrung rechtswidrigen Materials trifft, um von dem *safe harbor*-Privileg Gebrauch zu machen, erhält dieser entsprechend auch keine gesetzlich festgeschriebene Haftungsfreistellung.

Für den Host-Provider, der Material aufgrund einer *notification* gem. § 512 (c) (1) (C) DMCA entfernt oder sperrt, greift diese Freistellung lediglich, sofern er, nachdem er die *notification* erhalten hat, angemessene Schritte unternommen hat, um die *subscriber* darüber zu informieren, dass ihr Material gelöscht bzw. der Zugang hierzu gesperrt wurde und er nach Erhalt einer *counter notification* den Absender der *notification* hierüber informiert sowie das entsprechende Material gemäß den gesetzlichen Vorgaben ersetzt bzw. die Sperrung hierzu aufhebt.[1540]

i) Haftung für falsche Darstellung - Misrepresentations

§ 512 (f) DMCA enthält Bestimmungen zur Haftung im Falle von falschen Angaben im Rahmen der *notification* bzw. *counter-notification*. Demnach haftet jede Person, die wissentlich wesentlich falsche Angaben darüber macht, dass (1) Material oder eine Tätigkeit rechtsverletzend ist oder (2) Material oder eine Tätigkeit aufgrund eines Fehlers oder falschen Identifizierung entfernt bzw. blockiert wurde, für alle Schäden, inklusive Kosten und Anwaltsgebühren, welche dem behaupteten Rechtsverletzer, dem Urheberrechtsinhaber bzw. dessen autorisiertem Lizenznehmer oder dem ISP durch das Vertrauen auf die falschen Angaben und die entsprechende Löschung oder Sperrung bzw. die Aufhebung derselbigen entstand.

Nach der Gesetzesbegründung können vorsätzlich falsch gemachte Angaben gegenüber dem ISP für Rechteinhaber, ISP oder die Nutzer nachteilig sein, weshalb zur Verhinderung solcher Angaben diese Vorschrift eingefügt wurde.[1541]

---

take down in a good faith effort to comply with the requirements of new subsection (c) (1).“

[1540] § 512 (g) (1) und (2) DMCA.

[1541] H.R. Rep. 105-551(II), S. 59; S. Rep. 105-190, S. 49.

In *Online Piracy Group v. Diebold* beschäftigte sich der *N.D. California* mit der Frage, wann eine wissentliche und wesentliche *misrepresentation* vorliegt.[1542] Das Gericht führte zunächst aus, dass der Wortlaut der Vorschrift so klar und eindeutig sei, dass es keiner Übernahme irgendwelcher Standards aus einem anderen rechtlichen Kontext bedürfe.[1543] Eine wissentlich falsche Darstellung sei dann gegeben, wenn eine Person tatsächlich weiß, hätte wissen müssen oder, sofern sie in guten Glauben handelte, sie keine erheblichen Zweifel daran haben durfte, dass sie eine falsche Angabe macht.[1544] Bei der Bewertung des guten Glaubens sei insoweit auch bei einem auf IP-Recht spezialisiertem Anwalt kein strengerer Standard anzusetzen.[1545] Wesentlich bedeute, dass die falsche Angabe die Reaktion des ISP auf die DMCA *notification* beeinflusst, d.h. wenn dieser daraufhin das in der *notification* als rechtsverletzend behauptete Material entfernt oder den Zugang hierzu sperrt.[1546]

Eine wissentlich falsche Angabe innerhalb einer *counter notification* sah der *N.D. California* darin begründet, dass der Absender der *counter notification* vor Einleitung des *Notice and Takedown*-Verfahrens durch den Anwalt des Rechteinhabers mehrfach kontaktiert wurde und dieser ihm die zugrundeliegende geltend gemachte Urheberrechtsverletzung im Einzelnen näher erläuterte und erklärte.[1547]

aa) Dancing Baby-Entscheidung des Ninth Circuit

Der seit 2007 andauernde Rechtsstreit des sog. „*Dancing Baby"* erntete in den Medien sehr viel Aufmerksamkeit. Universal Music sendete eine Takedown-Notification an YouTube bzgl. des Videos

[1542] Online Policy Group v. Diebold, Inc., 337 F.Supp.2d 1195 (2004).
[1543] Online Policy Group v. Diebold, Inc., 337 F.Supp.2d 1195, 1204 (2004).
[1544] Online Policy Group v. Diebold, Inc., 337 F.Supp.2d 1195, 1204 (2004): „*'Knowingly' means that a party actually knew, should have known if acted with reasonable care or diligence, or would have had no substantial doubt had it been acting in good faith, that it was making misrepresentations."*.
[1545] Dudnikov v. MGA Entertainment, Inc., 410 F.Supp.2d 1010, 1013 (D. Colo. 2005).
[1546] Online Policy Group v. Diebold, Inc., 337 F.Supp.2d 1195, 1204 (2004):*„'Material' means that the misrepresentation affected the ISP's response to a DMCA letter"*.
[1547] Shropshire v. Canning, 809 F.Supp.2d 1139, 1148 (N.D. Cal. 2011).

eines Kleinkindes, welches zur Hintergrundmusik von Prince tanzend durch die Wohnung läuft.

Mitte 2015 traf der *Ninth Circuit* dann eine Grundsatzentscheidung, in dem er ausführte, dass der Absender einer *notification* zuvor zu berücksichtigen habe, ob es sich um einen Fall des *fair use* handele.[1548]

Das Gericht stellte zunächst fest, dass es sich bei einem Fall des *fair use* um eine gesetzliche Genehmigung zur Verwendung des Urheberrechtswerkes handele.[1549] Daher sei bei der Bewertung der Frage, ob der Urheberrechtsinhaber in gutem Glauben handelte, zu untersuchen, ob er vor Absendung der *notification* berücksichtigte, dass das streitgegenständliche Werk nicht unter die gesetzliche Ausnahmeregelung des *fair use* falle.[1550] Es führte aus, dass es nicht darauf ankomme, dass ein Gericht die Verwendung des urheberrechtlich geschützten Werkes als *fair use* ansehe, sondern darauf, dass der Urheberrechtsinhaber im guten Glauben dahingehend gehandelt habe, dass die Verwendung kein *fair use* darstelle.[1551] Der Urheberrechtsinhaber sei angehalten vor Absendung einer *notification fair use* in seiner Beurteilung des als urheberrechtsverletzend beanstandeten Materials zu berücksichtigen und müsse dahingehend in gutem Glauben sein, dass das Material nicht aufgrund der gesetzlicher Genehmigung im Sinne des *fair use* verwendet werden dürfe.[1552]

Entsprechend sei der Urheberrechtsinhaber nach § 512 (f) DMCA haftbar zu machen für falsche Angaben, sofern er vor Absendung der notification *fair use* nicht berücksichtigt habe.[1553] Sei er jedoch aufgrund einer vorherigen Prüfung der Auffassung, dass das als rechtsverletzend geltend Material kein *fair use* darstelle, hafte er nicht nach § 512 (f) DMCA, auch wenn das Gericht letzten Endes

[1548] Lenz v. Universal Music Corp., 801 F.3d 1126 (9th Cir. 2015).
[1549] Lenz v. Universal Music Corp., 801 F.3d 1126, 1132 (9th Cir. 2015).
[1550] Lenz v. Universal Music Corp., 801 F.3d 1126, 1134 (9th Cir. 2015).
[1551] Lenz v. Universal Music Corp., 801 F.3d 1126, 1134 (9th Cir. 2015).
[1552] Lenz v. Universal Music Corp., 801 F.3d 1126, 1134 (9th Cir. 2015).
[1553] Lenz v. Universal Music Corp., 801 F.3d 1126, 1135 (9th Cir. 2015).

zu einer anderen Beurteilung komme.[1554] Etwas anderes gelte jedoch, sofern der Urheberrechtsinhaber lediglich ein Lippenbekenntnis hierzu abgebe, es aber Beweise dafür gebe, dass er nicht in gutem Glauben handelte.[1555]

Nach Ansicht des *Ninth Circuit* kann zur Bestimmung, ob der Absender einer *notification* wissentlich falsche Angaben gemacht hat auch die *willful blindness*-Doktrin herangezogen werden.[1556] Hierfür müsste nachgewiesen werden, dass der Absender vor Versendung der *notification* (1) subjektiv von einer hohen Wahrscheinlichkeit ausging, dass das Werk von *fair use* gedeckt sei und (2) er bewusste Maßnahmen ergriff um eine diesbezügliche Kenntnis zu verhindern.[1557]

Hinsichtlich des Schadensersatzes, den der Betroffene unter § 512 (f) DMCA geltend machen kann, stellte der *Ninth Circuit* klar, dass hiervon nicht lediglich die unter § 512 (k) (1) (B) DMCA aufgeführten monetären Ansprüche zu fassen seien, die einen tatsächlich entstandenen Schaden bei dem Verletzten voraussetzen, sondern auch *nominal damages*.[1558] Bei no*minal damages* handelt es sich um einen geringfügigen Betrag, der dem Geschädigten zugesprochen wird, obwohl dieser keine tatsächlich zu beziffernde Schäden davongetragen hat.[1559]

Nachdem beide Parteien einen Antrag auf eine erneute Panel-Anhörung[1560] gestellt hatten, wies der *Ninth Circuit* diese Anfang 2016 zurück, änderte in der Folge aber sein Urteil aus 2015 in nicht unerheblicher Art und Weise.[1561]

[1554] Lenz v. Universal Music Corp., 801 F.3d 1126, 1135 (9th Cir. 2015).
[1555] Lenz v. Universal Music Corp., 801 F.3d 1126, 1135 (9th Cir. 2015).
[1556] Lenz v. Universal Music Corp., 801 F.3d 1126, 1136 (9th Cir. 2015).
[1557] Lenz v. Universal Music Corp., 801 F.3d 1126, 1136 (9th Cir. 2015).
[1558] Lenz v. Universal Music Corp., 801 F.3d 1126, 1137 (9th Cir. 2015).
[1559] Black's Law Dictionary „*Nominal damages are a trifling sum awarded to a plaintiff in an action, where there is no substantial loss or injury to be compensated, but still the law recognizes a technical invasion of his rights or a breach of the defendant's duty [...]*".
[1560] Sog. *Petition for Panel Rehearing*, geregelt in Rule 40 der Federal Rules of Appellate Procedure.
[1561] Lenz v. Universal Music Corp., D.C. No. 5:07-cv-03783-JF, filed September 14, 2015, amended March 17, 2016, abrufbar unter https://www.eff.org/document/ninth-circuit-amended-opinion, zuletzt besucht am 24.04.2016.

Während die 2015 Version des Urteils noch Ausführungen hinsichtlich der Bemühungen, die ein Urheberrechtsinhaber unternehmen müsse, um in gutem Glauben hinsichtlich der Berücksichtigung von *fair use* zu handeln, enthielt, fehlen diese in der geänderten Version 2016 gänzlich. So führte der Ninth Circuit 2015 aus, dass die Bemühungen des Urheberrechtsinhabers keine intensiven Untersuchungen erforderten.[1562] Da der Urheberrechtsinhaber ohnehin angehalten sei, sich vor Versendung einer *notification* das als rechtsverletzend behauptete Material anzusehen, wäre eine Berücksichtigung der Anwendbarkeit von *fair use* im Rahmen dieser Erstbegutachtung vollkommen ausreichend.[1563] In einem *obiter dictum* merkte das Gericht an, dass keine menschliche Überprüfung notwendig sei, sondern es vielmehr ausreiche, wenn ein Computer-Algorithmus so programmiert sei, dass er Fälle von *fair use* berücksichtige.[1564] Diesem Erfordernis sei bspw. Genüge getan, wenn das eingesetzte Computerprogramm automatisch Inhalte identifiziere, welche (1) die Videospur eines Videos mit derjenigen eines urheberrechtlich geschützten Werkes übereinstimme, (2) die Audiospur mit derjenigen desselben urheberrechtlich geschützten Werkes übereinstimme und (3) das Werk in seiner Gänze aus einem einzigen urheberrechtlich geschützten Werk bestehe.[1565] Hierunter würden beispielsweise urheberrechtlich geschützte Werke fallen, welche unverändert ins Internet gestellt werden. Der Urheberrechtsinhaber könnte dann Mitarbeiter einsetzen, die denjenigen Inhalt überprüfen, den ein Computerprogramm nicht in der Lage ist auszulesen.[1566] Das Gericht führte nicht weiter dazu aus, welcher Inhalt hiermit genau gemeint ist, es ist jedoch davon auszugehen, dass hierdurch bspw. Fälle ausgesondert werden sollten, in denen tatsächlich eine Einwilligung des Rechteinhabers

[1562] Lenz v. Universal Music Corp., 801 F.3d 1126, 1135 (9th Cir. 2015).
[1563] Lenz v. Universal Music Corp., 801 F.3d 1126, 1135 (9th Cir. 2015).
[1564] Lenz v. Universal Music Corp., 801 F.3d 1126, 1135 (9th Cir. 2015).
[1565] Lenz v. Universal Music Corp., 801 F.3d 1126, 1135 (9th Cir. 2015).
[1566] Lenz v. Universal Music Corp., 801 F.3d 1126, 1136 (9th Cir. 2015).

vorliegt, da das Computerprogramm nicht in der Lage ist eine solche Einschätzung vorzunehmen.[1567]

bb) Bewertung

Sowohl das Erfordernis zur Berücksichtigung von *fair use* als auch die Änderung des Urteils durch den *Ninth Circuit* sind zu begrüßen. Sie sind ein weiterer Stein auf dem Weg zu einer interessengerechten Lastenverteilung im Rahmen des DMCA *Notice and Takedown*-Verfahrens. Da das System des *Notice and Takedown* dem Absender der *notification* eine Art Vertrauensvorschuss[1568] zuspricht, ist es für den Erhalt des Gleichgewichts zwischen den verschiedenen Interessen von Bedeutung, dass dieser nicht unüberlegt und ohne ausreichende Prüfung *notifications* versendet. Die vorherige Prüfung, ob ein Fall des *fair use* vorliegt, ist ein wichtiger Bestandteil eines solchen Interessenausgleichs.

Auch die Auslassung der Ausführungen hinsichtlich der Art und des Umfangs einer Prüfung in dem geänderten Urteil von 2016 ist positiv zu bewerten. So ist insbesondere zu bezweifeln, dass ein Computerprogramm eine zutreffende Evaluation des *fair use* vornehmen kann.

cc) Fazit

§ 512 (f) DMCA steht in einem engen sachlichen Zusammenhang mit den *good faith*-Bestimmungen des § 512 (c) (3) (A) (v) DMCA und § 512 (g) (3) (C) DMCA. Sofern der ISP oder Nutzer in gutem Glauben gehandelt hat, kann ihm i.d.R. auch eine *material misrepresentation* nicht vorgeworfen werden.[1569] Es obliegt daher demjenigen, der eine *material misrepresentation* geltend macht,

[1567] So ist es beispielsweise auch schon vorgekommen, dass eine mit der Versendung von *notifications* beauftragte Agentur eine *notification* an Google sendete hinsichtlich Materials, dass sich auf der eigenen Webseite des Urheberrechtsinhabers befand, siehe auch Wiseman, 14 Nev. L.J. 210, 227 (2013).

[1568] So die Terminologie von Holznagel, S. 3.

[1569] So im Ergebnis auch Dudnikov v. MGA Entertainment, Inc., 410 F.Supp.2d 1010, 1012 (D. Colo. 2005).

nachzuweisen, dass kein *good faith* seitens der gegnerischen Partei vorlag, sondern diese wissentlich falsche Angaben gemacht hat.

Auch wenn die *Dancing Baby*-Entscheidung des *Ninth Circuit* einen wichtigen Beitrag zur Konkretisierung der Pflichten des Host-Providers vor Versendung einer *notification* geleistet hat, werden insbesondere die enge Auslegung des § 512 (f) DMCA und die Schwierigkeiten der Beweisführung als zu große Hürde für die Geltendmachung einer *material misrepresentation* angesehen.[1570] Zudem wird angeführt, dass die Rechtsprechung der Gerichte dazu führe, dass die Rechteinhaber vor Versendung einer *notification* keinen Anreiz hätten, eine sorgfältige Prüfung des als rechtsverletzend geltend gemachten Materials vorzunehmen oder angemessene Vorkehrungen zu treffen, um die Versendung einer fehlerhaften *notification* zu verhindern.[1571] Insbesondere fehle der Schutz vor dem Einsatz automatischer Software zum Auffinden rechtsverletzender Inhalte und der anschließend automatischen Versendung massenhafter ungeprüfter *notifications* an vermeintliche Rechtsverletzer.[1572]

Chen/Durkee/Friend/Urban schlagen daher vor, den Wortlaut des § 512 (f) DMCA so zu ändern, dass nicht von einer *substantial misrepresentation* sondern einer *reckless*[1573] *misrepresentation* die Rede ist.[1574] Hierdurch würde der Standard der *misrepresentation* herabgesetzt werden und damit der Urheberrechtsinhaber dazu angehalten, vor Versenden einer automatisch generierten *notification*, diese nochmals zu überprüfen.[1575]

Zudem plädieren sie für eine Aufnahme von *statutory damages* in § 512 (f) DMCA, da der tatsächlich erlittene ökonomische Schaden oftmals schwer zu beziffern sei.[1576] Dies würde auch die

[1570] Chen/Durkee/Friend/Urban, S. 9 f. (2011)
[1571] Chen/Durkee/Friend/Urban, S. 10 (2011).
[1572] Chen/Durkee/Friend/Urban, S. 11 (2011).
[1573] Deutsch: leichtsinnig, fahrlässig.
[1574] Chen/Durkee/Friend/Urban, S. 12 (2011).
[1575] Chen/Durkee/Friend/Urban, S. 12 (2011).
[1576] Chen/Durkee/Friend/Urban, S. 14 (2011).

Versendung fehlerfreier *notifications* fördern und vor der unbedachten Versendung fehlerhafter *notifications* abschrecken.[1577]

j) Anordnung zur Identifizierung des Rechtsverletzers

Dem Urheberrechtsinhaber bzw. einer von ihm autorisierten Person steht gem. § 512 (h) (1) DMCA die Möglichkeit offen, gegen den ISP eine strafbewehrte Anordnung (*subpoena*) zur Identifizierung des behaupteten Rechtsverletzers zu erlangen. Der Antrag zum Erlass einer entsprechenden *subpoena* muss beim *clerk* des jeweils zuständigen *district courts* eingereicht werden und eine Kopie der *notification* enthalten[1578], die beantragte *subpoena*[1579] sowie eine eidesstattliche Erklärung darüber, dass der Zweck der *subpoena* darin liegt, Informationen über die Identität des behaupteten Rechtsverletzers zu erlangen und diese Informationen lediglich für den Schutz der Urheberrechte genutzt werden[1580].

Der Inhalt der *subpoena* ist in § 512 (h) (3) DMCA festgeschrieben. Danach soll diese den ISP, welche die *subpoena* erhält, autorisieren und anweisen dem Urheberrechtsinhaber zügig ausreichende Informationen mitzuteilen, die es ihm ermöglichen, den behaupteten Rechtsverletzer zu identifizieren, vorausgesetzt, der ISP verfügt über diese Informationen. Nach den Gesetzgebungsmaterialien soll hierdurch sichergestellt werden, dass nur solche Informationen herauszugeben sind, die der Provider besitzt und ihn keine Pflicht zur Durchführung von Recherchen zum Auffinden anderer Informationen trifft.[1581]

Erfüllt die *notification* die Voraussetzungen des § 512 (c) (3) (A) DMCA und ist die *subpoena* formgerecht sowie die eidesstattliche Erklärung ordnungsgemäß ausgefertigt, hat der *clerk* die beantragte *subpoena* zügig auszustellen, zu unterzeichnen und dem Antragsteller zurückzusenden.[1582] Eine inhaltliche Prüfung hinsichtlich der Begründetheit der geltend gemachten

[1577] Chen/Durkee/Friend/Urban, S. 13 (2011).
[1578] § 512 (h) (2) (A) DMCA.
[1579] § 512 (h) (2) (B) DMCA.
[1580] § 512 (h) (2) (C) DMCA.
[1581] H.R. Rep. 105-551(II), S. 61; S. Rep. 105-190, S. 52.
[1582] § 512 (h) (4) DMCA.

urheberrechtlichen Ansprüche findet somit nicht statt. Entsprechend führen auch der *House* und *Senate Report* aus, dass die Ausfertigung der Anordnung eine amtliche Tätigkeit sei, die schnell durchzuführen ist.[1583]

Nach Erhalt der *subpoena* hat der ISP dem Urheberrechtsinhaber zügig die darin verlangten Informationen mitzuteilen, unabhängig davon, ob er auf die *notification* reagiert.[1584] Dies bedeutet, dass selbst wenn der ISP sich dazu entscheidet, die in der *notification* beanstandete Rechtsverletzung nicht zu entfernen oder zu sperren, er dennoch die Informationen über den behaupteten Rechtsverletzer herausgeben muss.[1585] Eine Benachrichtigung des behaupteten Rechtsverletzers darüber, dass Informationen über seine Identität herausgegeben wurden, ist hingegen nicht vorgesehen.[1586]

Der Erlass, die Zustellung und die Durchsetzung der *subpoena* richten sich im Übrigen nach Rule 45 der *Federal Rules of Civil Procedure*.[1587]

Umstritten ist, ob diese Bestimmung für alle vier ISP beansprucht werden kann. Die h.M. geht davon aus, dass diese lediglich Anwendung findet für Cache- und Host-Provider sowie *Information Location Tools*.[1588] Hintergrund hierfür ist die explizite Inkorporierung der *notification* gem. § 512 (c) (3) (A) DMCA in § 512 (h) DMCA. Anders als § 512 (b), (c) und (d) DMCA enthält § 512 (a) DMCA kein entsprechendes *Notice and Takedown*-Verfahren. Auch die Gesetzgebungsmaterialien sprechen für eine

---

[1583] H.R. Report 105-551 (II), S. 61; S. Rep. 105-190, S. 51:*"The issuing of the order shall be a ministerial function performed quickly for this provision to have its itended effect."*

[1584] § 512 (h) (5) DMCA.

[1585] Nimmer, § 12B.09 [A] [1].

[1586] Nimmer, § 12B.09 [A] [1].

[1587] § 512 (h) (6) DMCA.

[1588] Recording Industry Association of America, Inc., v. Verizon Internet Services, Inc., 351 F.3d 1229, 1234f. (D.C. Cir. 2003); In re Charter Communications, Inc., Subpoena Enforcement Matter, 393 F.3d 771, 777 (8th Cir. 2005); In re Subpoena to Univ. of N.C. at Chapel Hill, 367 F. Supp. 2d 945, 952 (M.D.N.C. 2005); Nimmer, § 12B.09 [A] [2]; Bridy, 13 Vand. J. Ent. & Tech. L. 695, 718 (2011); a.A.:Mtima, 61 Rutgers L. Rev. 627, 704 (2009). Wenngleich diese Regelung im Hinblick auf den Cache-Provider und die *Information Location Tools* eher theoretischer Natur sein dürfte, da diese i.d.R. nicht über entsprechende Informationen eines behaupteten Rechtsverletzers verfügen.

entsprechende Unanwendbarkeit auf den Access-Provider. So ist hier die Rede von der Möglichkeit einer Anordnung für Urheberrechtsinhaber, welche eine *notification* eingereicht haben oder eine solche noch einreichen wollen.[1589]

Wie der *D.C. Circuit* ausgeführt hat, ist es durchaus denkbar, dass der Kongress den § 512 (h) DMCA anders gestaltet hätte, wenn damals bereits die Peer-to-Peer Technologie existiert hätte.[1590] Wie der *D.C. Circuit* jedoch weiter erörtert, liegt es nicht in der Kompetenz der Gerichte, die geltenden *safe harbor*-Bestimmungen umzuschreiben und entgegen dem klaren Wortlaut auf § 512 (a) DMCA anzuwenden.[1591]

Der Urheberrechtsinhaber hat folglich keine Möglichkeit zum Erlass einer *subpoena* gegen den Access-Provider gem. § 512 (a) DMCA.

Die praktischen Folgen einer solchen Interpretation für den Urheberrechtsinhaber nennt Judge Murphy in ihrer abweichenden Urteilsbegründung (*dissent*) im „Charter Communications"-Fall.[1592] Ohne die Möglichkeit des Erhalts einer *subpoena* nach § 512 (h) DMCA ist der Rechteinhaber dazu angehalten, John Doe Klagen[1593] einzureichen, was nicht nur kostspielig sondern auch zeitaufwändig ist.[1594]

[1589] H.R. Report 105-551 (II), S. 60; S. Rep. 105-190, S. 51: *"New Section 512(g) creates a procedure by which copyright owners or their authorized agents who have submitted or will submit a request for notification satisfying the requirements of new subsection (c)(3)(A) may obtain an order for identification of alleged infringers who are users of a service provider's system or network."*

[1590] So Recording Industry Association of America, Inc., v. Verizon Internet Services, Inc., 351 F.3d 1229, 1238 (D.C. Cir. 2003); Bridy, 13 Vand. J. Ent. & Tech. L. 695, 719 (2011).

[1591] Recording Industry Association of America, Inc., v. Verizon Internet Services, Inc., 351 F.3d 1229, 1238 (D.C. Cir. 2003); Bridy, 13 Vand. J. Ent. & Tech. L. 695, 719 (2011).

[1592] In re Charter Communications, Inc., Subpoena Enforcement Matter, 393 F.3d 771, 782 (8th Cir. 2005) (Murphy, J., dissenting).

[1593] Eine Klage gegen John Doe (*John Doe lawsuit*) wird in den USA eine Klage gegen Unbekannt genannt. Auf den Vorteil einer John Doe Klage weist *Lemley* hin, welcher darin besteht, dass der Rechteinhaber erstmal hinsichtlich der Begründetheit seines Anspruchs ausführen und darlegen muss bevor die Identität des vermeintlichen Rechtsverletzers preisgegeben wird, siehe Lemley, 6 J. Telecomm. & High Tech. L. 101, 117 (2007).

[1594] In re Charter Communications, Inc., Subpoena Enforcement Matter, 393 F.3d 771, 782 (8th Cir. 2005) (Murphy, J., dissenting).

Diese Nachteile des Urheberrechtsinhabers werden allerdings durch die berechtigten Interessen der Nutzer an ihrer Privatsphäre wieder aufgewogen. Anders als bei den anderen ISP hat der Urheberrechtsinhaber gegenüber dem Access-Provider keine effektive andere Möglichkeit zur Bekämpfung einer Urheberrechtsverletzung, welche über das System des Access-Providers vorgenommen wird. Während er bei den anderen ISP das Instrument der *notification* nutzen kann, um eine behauptete Rechtsverletzung auf einfache Art und Weise zu beseitigen, fehlt es ihm an einer entsprechenden Möglichkeit gegenüber dem Access-Provider. Der Access-Provider genießt von allen ISP die weitgehendste Privilegierung, da er in der Regel lediglich die technische Infrastruktur zur Übermittlung von Informationen zur Verfügung stellt. Könnte der Urheberrechtsinhaber nun durch Ausfertigung einer *subpoena* im Rahmen des § 512 (h) DMCA den Access-Provider dazu verpflichten, aufgrund einer behaupteten Rechtsverletzung Auskunft über seine Nutzer zu geben, würde dies die Interessen der Nutzer erheblich beeinträchtigen. Eine solche Einschränkung ist bereits vor dem Hintergrund, dass die Ausfertigung der *subpoena* keinerlei materiell-rechtliche Prüfung des behaupteten Anspruchs des Urheberrechtsinhabers beinhaltet, nicht gerechtfertigt.

Mit dieser Interpretation im Einklang steht auch die Tatsache, dass es dem Rechteinhaber gem. § 512 (j) (1) (B) DMCA unbenommen bleibt, eine *injunction* in Form des Ausschlusses des Rechtsverletzers bzw. die Zugangssperrung zu Material, welches sich außerhalb der USA befindet, gerichtlich geltend zu machen. Im Rahmen der Geltendmachung einer entsprechenden Anordnung wird das Gericht dann u.a. auch den urheberrechtlichen Anspruch des Urheberrechtsinhabers prüfen. Fehl geht hier die Auffassung von *Mtima*, dass, um eine *injunction* nach § 512 (j) DMCA zu erhalten, dem Urheber die Identität des Nutzers bekannt sein

müsse.[1595] Die injunction des § 512 (j) DMCA richtet sich ja gerade gegen den ISP und eben nicht gegen den direkten Rechtsverletzer.

6. Umfang der Privilegierung

Fallen die ISP unter den Anwendungsbereich der *safe harbor,* sind sie von monetären Klagebegehren (*monetary relief*) generell befreit.[1596] Nach der Legaldefinition des DMCA fallen unter den Begriff der *monetary relief* Schadensersatz, Kosten, Anwaltskosten und jede weitere Form von monetärer Zahlung.[1597] Im Falle von sonstigen Anordnungen, wie beispielsweise Anordnungen auf Unterlassung, sind die potentiellen Ansprüche durch § 512 (j) DMCA beschränkt. § 512 (j) DMCA stellt daher keine Anspruchsgrundlage für den Erlass einer Anordnung dar für den Fall, dass der ISP für eine Urheberrechtsverletzung als *secondary infringer* verantwortlich ist. Die allgemeine Anspruchsgrundlage für Anordnungen jeglicher Art findet sich in 17 U.S.C. § 502.

§ 512 (j) DMCA unterscheidet bei der Art der möglichen Anordnungen zwischen dem Cache-, Host-Provider und *Information Location Tools* auf der einen Seite sowie dem Access-Provider auf der anderen Seite.

Vor dem Erlass jeglicher Anordnung schreibt das Gesetz dem Gericht zusätzlich anzustellende Überlegungen vor, welche über die nach geltendem Recht existierenden hinausgehen und welche das Gericht dazu anhalten, Faktoren zu berücksichtigen, die spezifische Bedeutung für die digitale Online-Umgebung haben.[1598]

Das Gericht hat gem. § 512 (j) (2) (A) DMCA zu erwägen, ob die Anordnung den ISP oder den Betrieb seines Systems oder Netzwerkes wesentlich beeinträchtigen würde. Zudem hat es das Ausmaß des Schadens, welcher der Urheberrechtsinhaber voraussichtlich erleidet, sofern keine Schritte unternommen werden, um die Rechtsverletzung zu verhindern oder zu

[1595] Mtima, 61 Rutgers L. Rev. 627, 669 (2009).
[1596] Dies gilt gleichermaßen für Access-, Cache- und Host-Provider sowie für Information Location Tools, siehe § 512 (a), (b), (c) und (d) DMCA:*„A service provider shall not be liable for monetary relief [...].“*
[1597] § 512 (k) (2) DMCA.
[1598] H.R. Rep. 105-551(II), S. 63; S. Rep. 105-190, S. 53.

unterlassen, gem. § 512 (j) (2) (B) DMCA zu berücksichtigen. Nach § 512 (j) (2) (C) DMCA hat es weiterhin zu erwägen, ob die Umsetzung einer solchen Anordnung technisch möglich und effektiv ist und nicht den Zugang zu rechtmäßigem Material beeinträchtigt. Nach dieser Überlegung wäre es denkbar, dass eine Anordnung unter dem Gesichtspunkt vereitelt werden kann, dass der Zugang zu rechtsverletzendem Material so weit verbreitet ist, dass eine Anordnung gegen einen einzelnen ISP der Anforderung der Effektivität nicht entspricht und daher eine Verfolgung der Rechtsverletzung an der Quelle erfolgversprechender sein könnte. Zuletzt ist nach § 512 (j) (2) (D) DMCA zu prüfen, ob es andere weniger belastende und gleichermaßen effektive Maßnahmen zur Verhinderung oder Unterlassung des Zugangs zu rechtsverletzendem Material gibt.

Zudem ist eine Anordnung prinzipiell lediglich nach Mitteilung an den ISP möglich und sofern diesem die Möglichkeit des Erscheinens eingeräumt wird.[1599] Entsprechend sind *ex parte* Unterlassungsanordnungen[1600], wie bspw. *temporary injunctions*[1601], gegen einen ISP der unter den *safe harbor* Schutz fällt, nicht möglich.[1602]

Die *safe harbor*-Bestimmungen des DMCA gewähren hingegen keinen Schutz vor strafrechtlicher Verantwortlichkeit des ISP.[1603]

[1599] § 512 (j) (3) DMCA.

[1600] Ex parte Anordnungen werden von dem Gericht ohne vorherige Anhörung der anderen Partei erlassen.

[1601] *Temporary injunctions* sind Anordnungen, welche bestimmte Handlungen zur Vermeidung von *irreparable injury* (irreparabler Schäden) für den Antragsteller untersagen. Sie können vom Gericht auf Antrag einer Partei erlassen werden. Siehe hierzu ausführlich Nimmer on Copyright, § 14.06 [A].

[1602] H.R. Rep. 105-551(II), S. 63; S. Rep. 105-190, S. 53; mit Ausnahme von Anordnungen zur Beweissicherung oder anderweitigen Anordnungen, welche keinen nachteiligen Effekt auf den Betrieb des Kommunikationsnetzwerkes des ISP haben, diese sind ausdrücklich gem. § 512 (j) (3) DMCA hiervon ausgenommen.

[1603] Nimmer on Copyright, § 12.B.01 [C] [2], der darauf hinweist, dass für eine strafrechtliche relevante Urheberrechtsverletzung ohnehin Vorsatz vorausgesetzt wird.

a) Host-, Cache-Provider und Information Location Tools

Gem. § 512 (j) (1) (A) DMCA kann ein Gericht gegen den Host- und Cache-Provider sowie die *Information Location Tools* lediglich drei verschiedene Anordnungen erlassen.

aa) Entfernung/Sperrung

Das Gericht kann gem. § 512 (j) (1) (A) (i) DMCA eine Verfügung erlassen, die es dem Provider auferlegt, das rechtsverletzende Material, welches sich auf einer spezifischen Online-Seite des Systems oder Netzwerks des ISP befindet, zu entfernen bzw. den Zugang hierzu zu sperren. Diese Verfügung entspricht der in § 512 (b) (2) (E), 512 (c) (1) (C) und § 512 (d) (3) DMCA geregelten Entfernung bzw. Sperrung urheberrechtswidriger Inhalte.

bb) Ausschluss des Rechtsverletzers

Das Gericht kann ferner gem. § 512 (j) (1) (A) (ii) DMCA anordnen, dass der ISP das Konto des *subscribers* bzw. *account holders* zu kündigen hat.

cc) Sonstige notwendige Anordnungen

Zudem kann ein Gericht gem. § 512 (j) (1) (A) (iii) DMCA weitere Anordnungen treffen, die es für notwendig hält, um Urheberrechtsverletzungen auf einem spezifischen Online-Speicherplatz zu verhindern oder zu unterlassen, sofern eine solche Anordnung die am wenigsten belastende unter den verfügbaren und gleichermaßen effektiven Anordnungen darstellt. Es ist unklar, welche Anordnungen dies umfassen könnte. Nach *Nimmer* ist es dem Gericht aber bereits untersagt eine entsprechende Anordnung zu erlassen, sofern eine effektive Anordnung gegen den direkten Verletzer erlassen werden kann.[1604]

b) Access-Provider

Dem Gericht stehen gegen den Access-Provider gem. § 512 (j) (1) (B) DMCA lediglich zwei potentielle Anordnungen zur Verfügung.

[1604] Nimmer on Copyright, § 12B.11 [A] [2].

aa) Ausschluss des Rechtsverletzers

Gem. § 512 (j) (1) (B) (i) DMCA kann ein Gericht den Access-Provider durch eine Anordnung verpflichten, das Konto eines *subscribers* bzw. *account holders* zu kündigen.

bb) Sperrverfügung

Das Gericht hat gem. § 512 (j) (1) (B) (ii) DMCA weiterhin die Möglichkeit eine Anordnung gegen den Access-Provider zu erlassen, die es ihm untersagt, den Zugang zu einem spezifischen, identifizierten Online-Speicherplatz durch angemessene Schritte zu gewähren. Dies gilt allerdings nur, sofern sich dieser Online-Speicherplatz außerhalb der USA befindet. Laut dem *House* und *Senate Report* sind solche Anordnungen nicht verfügbar gegen eine Seite, die sich innerhalb der USA befindet.[1605]

Hierdurch wird die US-amerikanische Zuständigkeit auf Inhalte ausgedehnt, die in den USA als urheberrechtsverletzend eingestuft werden, unabhängig davon, ob diese sich auf einem Server in einem Land befinden könnten, in dem kein entsprechender Urheberrechtsschutz für die gegenständlichen Inhalte besteht.[1606]

Soweit ersichtlich, beschäftigte sich bislang lediglich ein Fall mit einer entsprechenden Anordnung. In *Arista Records v. AT&T Broadband* verklagten mehrere Plattenfirmen einen Access-Provider und verlangten von diesem die Sperrung einer ausländischen Webseite auf Grundlage von § 512 (j) (1) (B) (ii) DMCA.[1607] Sie versäumten aber hinsichtlich der Verantwortlichkeit des Access-Providers nach den allgemeinen Grundsätzen auszuführen und gingen irrigerweise davon aus, dass eine Anordnung zur Sperrung unabhängig von einer Verantwortlichkeit als *direct* oder *indirect infringer* gegeben sei. Das Gericht hatte jedoch keine Gelegenheit die Begründetheit des Falls zu prüfen, da die beanstandete Webseite weniger als eine Woche nach

[1605] H.R. Rep. 105-551(II), S. 63; S. Rep. 105-190, S. 53.
[1606] Ballon, 4.12[11].
[1607] Arista Records, Inc. v. AT&T Broadband Corp., No. 02-CV-6554 (S.D.N.Y. filed Aug. 16, 2002).

Klageeinreichung offline ging und die Klage entsprechend zurückgenommen wurde.[1608]

c) Fazit

Anordnungen gegen ISP scheinen in der Praxis keine Rolle zu spielen.[1609] Dies mag auch daran liegen, dass die nach § 512 (j) möglichen Anordnungen bereits durch entsprechende Bestimmungen des DMCA größtenteils abgedeckt werden und somit vorgerichtlich bereits umgesetzt werden. So ist eine Entfernung des rechtsverletzenden Materials wie sie § 512 (j) (1) (A) (i) DMCA vorsieht, oftmals bereits durch ein erfolgreiches *Notice and Takedown*-Verfahren umgesetzt worden. Eine Kündigung des Nutzerkontos durch den Host- oder Access-Provider gem. § 512 (j) (1) (A) (ii) DMCA bzw. § 512 (j) (1) (B) (i) DMCA kann der ISP bereits über die entsprechend nach § 512 (i) (1) (A) DMCA implementierte *repeat infringer policy* vornehmen. Weitere Anordnungen werden in der Praxis oftmals daran scheitern, dass eine direkte Inanspruchnahme des Rechtsverletzers möglich ist. Insoweit konstituieren § 512 (j) (1) (A) (iii) DMCA und § 512 (j) (2) (D) DMCA, welche die Berücksichtigung anderer, für den ISP weniger belastenden und gleichermaßen effektiven Maßnahmen, vorschreiben, letzten Endes eine Subsidiarität der Providerhaftung.

Entsprechend führte auch der *N.D. California* in *Io Group v. Veoh* aus, dass, da Veoh für sich die *safe harbor*-Privilegien in Anspruch nehmen könne, der einzig mögliche Anspruch gegenüber Veoh der einer Anordnung unter § 512 (j) DMCA sei.[1610] Da Veoh im vorliegenden Fall jedoch alle rechtsverletzenden Inhalte gelöscht habe und solche Inhalte auch nicht mehr auf seiner Webseite erlaube, wären jegliche Ansprüche zu denen Io berechtigt wäre, ohnehin hinfällig.[1611]

[1608] Kopko, 8 Computer L. Rev. & Tech. J. 83, 84 (2003).
[1609] So auch Holznagel, S. 49.
[1610] Io Group, Inc. v. Veoh Networks, Inc., 586 F.Supp.2d 1132, 1154 (N.D.Cal. 2008).
[1611] Io Group, Inc. v. Veoh Networks, Inc., 586 F.Supp.2d 1132, 1154 (N.D.Cal. 2008).

7. Ergebnis

Die Stimmen im Schrifttum sind geteilter Meinung dahingehend, ob mit den *safe harbor*-Privilegien des DMCA die Ziele der Schaffung von Rechtssicherheit für die ISP, der Förderung von Online-Innovationen sowie des effektiven Schutzes von Urheberrechten erreicht wurden.[1612]

Die wohl h.M. ist jedoch der Auffassung, dass der *safe harbor* maßgeblich zu der Entwicklung neuer innovativer Internetdienste beitragen hat.[1613]

Als Erfolg kann sicherlich gewertet werden, dass eine Großzahl der DCMA Fälle im Rahmen von sog. *summary judgements motions*[1614] entschieden werden.[1615] Durch diesen vorprozessualen Antrag können gesamte Rechtsstreitigkeiten oder lediglich einzelne Aspekte ohne Gerichtsverhandlung entschieden werden unter der Voraussetzung, dass (1) es keine strittigen materiellen Fakten gibt und (2) die antragsstellende Partei zu einem Urteil von Rechts wegen berechtigt ist.[1616] Dieses Verfahren ist sowohl kostengünstiger als auch schneller und bewahrt somit die Parteien vor den hohen Prozesskosten, die ein gewöhnliches gerichtliches Verfahren üblicherweise mit sich bringt. Dies ist vor allem vor dem Hintergrund bedeutsam, dass im US-amerikanischen Recht jede Partei üblicherweise selbst ihre Prozess- und Anwaltskosten trägt und es gem. 17 U.S.C. § 505 im Ermessen des Gerichts steht, eine entgegenstehende Kostenentscheidung zu treffen. *Blevins* weist insofern zurecht daraufhin, dass das Obliegen in einem Rechtsstreit nicht das Wichtigste ist, da selbst in diesem Falle, die horrenden

---

[1612] Dafür: Carroll, U. Miami L. Rev. 421, 443 (2014); Mlynar, 19 Intell. Prop. L. Bull. 1, 1 (2014); Notice and Takedown in Everyday Practice, S. 115; Wiseman, 14 Nev. L.J. 210, 215 (2013); Zweifelnd: Cooley, 64 SMU L. Rev. 691, 708 (2011); Reese, 34 Sw. U. L. Rev. 287, 323 (2004); Weinstein, 26 Cardozo Arts & Ent. L.J. 598, 620 f. (2008); Dagegen: Helman/Parchomovsky, 111 Colum. L. Rev. 1194, 1205 (2011).

[1613] Carroll, U. Miami L. Rev. 421, 443 (2014); Mlynar, 19 Intell. Prop. L. Bull. 1, 1 (2014); Wiseman, 14 Nev. L.J. 210, 215 (2013).

[1614] Gesetzlich geregelt in Rule 56 Federal Rules of Civil Procedure.

[1615] Ballon, 4.12[1].

[1616] Rule 56 (a) Federal Rules of Civil Procedure: *„A party may move for summary judgment [...]. The court shall grant summary judgment if the movant shows that there is no genuine dispute as to any material fact and the movant is entitled to judgment as a matter of law. [...].“*

Kosten des Gerichtsverfahren den ISP in den Ruin treiben können.[1617]

Vor diesem Hintergrund plädiert *Blevins* für die Schaffung von *bright-line rules* (klaren Regeln) bei der gerichtlichen Interpretation des § 512 DMCA.[1618] Denn um einem vorgerichtlichen *summary judgement* zu entkommen und damit eine Verhandlung im ordnungsgemäßen Verfahren einzuleiten genüge oftmals schon die Begründung von Unklarheiten hinsichtlich einer der vielen gesetzlichen Voraussetzungen des § 512 DMCA.[1619]

Hauptaugenmerk der öffentlichen Debatte liegt auf der Haftung des Host-Providers, insbesondere auf dem für diesen anwendbaren *Notice and Takedown*-Verfahren. Hauptkritikpunkt an dem derzeitigen System des DMCA ist die zu leichte Entfernung behaupteter Rechtsverletzungen durch den Urheberrechtsinhaber und damit eine Gefährdung der *free speech*.[1620] Es wird insbesondere kritisiert, dass das Verfahren die ISP dazu veranlasst, vorschnell, auch bei unseriösen *notifications*, Material zu entfernen.[1621] Entsprechend würden die Urheberrechtsinhaber gegenüber den Nutzern, die Inhalte anbieten, bevorteilt.[1622]

Das *Notice and Takedown*-Verfahren verlangt keine Prüfung des Sachverhaltes oder der Begründetheit der der *notification* zugrunde liegenden behaupteten Rechtsverletzung.[1623] Der ISP muss lediglich schematisch die Befolgung der formellen Anforderungen an die *notification* und die *counter notification* prüfen.[1624] Nimmt der ISP dennoch eine inhaltliche Prüfung der beanstandeten

---

[1617] Blevins, 34 Cardozo L. Rev. 1821, 1823 (2013); so beispielsweise Veoh, die trotz Obsiegens vor dem *Ninth Circuit* in Konkurs gingen.
[1618] Blevins, 34 Cardozo L. Rev. 1821, 1825 f. (2013).
[1619] Blevins, 34 Cardozo L. Rev. 1821, 1837 (2013).
[1620] Lemley, 6 J. Telecomm. & High Tech. L. 101, 114 f. (2007); Walker, Virginia Journal of Law & Technology Vol. 9, No.2., 27.
[1621] So bspw. Lemley, 6 J. Telecomm. & High Tech. L. 101,114 f. (2007); Murtagh, 61 Hastings L.J. 233, 256 (2009).
[1622] Blom, 1 Case W. Reserve J.L. Tech. & Internet 36, 54 (2009).
[1623] Insoweit falsch Klemchuk/Jones, 18 No. 10 J. Internet L.1, 35, 36 (2015), welche ausführen, dass der ISP nach Erhalt einer notification „*[...] must evaluate the merit of the request or perhaps consult with legal counsel.*"
[1624] Ballon, 4.12[9][C].

Rechtsverletzung vor, riskiert er hierdurch den Verlust seiner *safe harbor*-Privilegierung, bspw. wenn die Prüfung längere Zeit in Anspruch nimmt und hierdurch entsprechend eine Löschung bzw. Sperrung des Inhalts nicht mehr als *expeditious* betrachtet werden kann.

In der Praxis ist es dennoch insbesondere bei UGC-Plattformen durchaus üblich, dass die eingehenden *notifications* auch hinsichtlich ihrer materiell-rechtlichen Grundlage einer Prüfung unterzogen werden und gegebenenfalls von den ISP auch zurückgewiesen werden.[1625] Grund hierfür sind die negativen Auswirkungen, die eine unberechtigte Löschung von Nutzermaterial mit sich bringen kann.[1626] Eine rechtliche Pflicht trifft den ISP allerdings nicht.

Zudem versuchen Rechteinhaber unzulässigerweise immer wieder sowohl eine Anordnung zur Identifizierung des Rechtsverletzers gegenüber dem Access-Provider zu erlangen als auch das *Notice and Takedown*-Verfahren gegenüber diesem anzuwenden.[1627]

Weiterhin wird bemängelt, dass auch im Falle einer *counter-notification* das als rechtsverletzend beanstandete Material zunächst für mindestens 10 Tage offline ist.[1628] Dies ist besonders kritisch zu sehen bei zeitkritischen Materialien, wie aktuellen Nachrichten oder Inhalten zu politischen Kampagnen.[1629]

Zudem führt das *Notice and Takedown*-Verfahren dazu, dass das Material, auch im Falle einer Klageerhebung nach *counter notification*, so lange offline bleibt, bis das Gericht ein entgegenstehendes Urteil fällt. Im Gegensatz dazu bleibt das als rechtsverletzend geltend gemachte Material während einer

[1625] Notice and Takedown in Everday Practice, S. 40 ff.
[1626] Notice and Takedown in Everday Practice, S. 41.
[1627] Murtagh, 61 Hastings L.J. 233, 254 (2009); Urban/Quilter, 22 Santa Clara Computer & High Tech. L.J. 621, 644 (2006).
[1628] Holznagel, S. 55; Chen/Durkee/Friend/Urban, S. 16 f. (2011); Pollack, 22 Santa Clara High Tech. L.J. 547, 561 (2005); Urban/Quilter, 22 Santa Clara Computer & High Tech. L.J. 621, 636 f. (2006).
[1629] Chen/Durkee/Friend/Urban, S. 3 (2011).

Urheberrechtsklage abseits des DMCA so lange online bis das Gericht ein gegenteiliges Urteil fällt.[1630]

Auch hinsichtlich der *Information Location Tools* erfährt das *Notice and Takedown*-System berechtigterweise Kritik, fehlt es hier doch an wirksamen Mechanismen für den betroffenen Inhalteanbieter seine Rechte hinsichtlich der unberechtigten Entfernung eines Links geltend zu machen.[1631]

Die anhaltende Kritik am derzeitigen System des § 512 DMCA mag auch der Grund dafür gewesen sein, dass das *U.S. Copyright Office* am 31. Dezember 2015 eine *notice of inquiry* hinsichtlich des § 512 DMCA veröffentlichte.[1632] Die „*Section 512 Study: Notice and Request for Public Comment*" soll laut eigener Darstellung die Auswirkungen und die Effektivität der DMCA *safe harbor*-Bestimmungen untersuchen. Als Schwerpunkte der Untersuchung hat das *U.S. Copyright Office* die bereits zuvor vermehrt im Schrifttum geäußerten Kritikpunkte festgelegt. So besteht der insgesamt 30 Fragen umfassende Katalog aus den folgenden acht Unterkategorien: (1) *General Effectiveness of Safe Harbors*, (2) *Notice and Takedown Process*, (3) *Counter Notification*, (4) *Legal Standards* (*actual, red flag knowledge, financial benefit, right and ability to control*), (5) *Repeat Infringers*, (6) *Standard Technical Measures*, (7) *Remedies* (*limited injunctive relief, remedies for misrepresentation*), (8) *Other Issues*.

Die Öffentlichkeit hatte bis zum 01. April 2016 Gelegenheit zu allen oder einzelnen Fragen schriftlich Stellung zu nehmen. In diesem Zeitraum erhielt das *U.S. Copyright Office* 92.400 Stellungnahmen, welche vom *U.S. Copyright Office* öffentlich zugänglich gemacht wurden.[1633] Im Mai wurden diesbezüglich auch

---

[1630] Ballon, 4.12[12].

[1631] So z.B. Urban/Quilter, 22 Santa Clara Computer & High Tech. L.J. 621, 690 (2006).

[1632] 81862 Federal Register / Vol. 80, No. 251 / Thursday, December 31, 2015 / Notices, Docket No. 2015-7, abrufbar unter http://copyright.gov/fedreg/2015/80fr81862.pdf, zuletzt besucht am 24.04.2016.

[1633] Einsehbar unter https://www.regulations.gov/docketBrowser?rpp=25&so=ASC&sb=title&po=0&dct=PS&D=COLC-2015-0013&refD=COLC-2015-0013-0002, zuletzt besucht am 28.08.2016.

öffentliche Diskussionsrunden (*public roundtables*) in San Francisco und New York abgehalten.[1634]

8. Verbesserungsvorschläge

Das Schrifttum hat in den vergangenen Jahren vielfach Verbesserungsvorschläge der bestehenden Regelungen des § 512 DMCA hervorgebracht. Im Folgenden werden die bedeutendsten dargestellt.

a) Eidesstattliche Versicherung des guten Glaubens

Zunächst wird vorgeschlagen, die Anforderungen an die *notification* den Anforderungen an die *counter notification* anzupassen.[1635] Entsprechend sollte auch in § 512 (c) (3) (A) (vi) DMCA eine Pflicht zur eidesstattlichen Versicherung hinsichtlich der Korrektheit der Angaben bzw. des guten Glaubens des Absenders in der *notification* aufgenommen werden.

b) Verzögerung des Takedown

Um einem Missbrauch *des Notice and Takedown*-Verfahrens zu begegnen, sollen die im Rahmen einer *notification* beanstandeten Materialien erst dann entfernt bzw. gesperrt werden, wenn der vermeintliche Rechtsverletzer die Möglichkeit hatte, eine *counter notification* einzureichen.[1636] Die Einführung einer bestimmten Frist, innerhalb welcher der behauptete Rechtsverletzer eine *counter notification* einreichen kann, hat allerdings den Nachteil, dass hierdurch die durch das *Notice and Takedown*-Verfahren beabsichtigte schnelle Abhilfe für den Urheberrechtsinhaber erheblich beeinträchtigt werden würde.[1637]

Daher wird an anderer Stelle vorgeschlagen, dem Urheberrechtsinhaber die Pflicht aufzuerlegen, eine Kopie der

---

[1634] Siehe http://www.copyright.gov/policy/section512/, zuletzt besucht am 28.08.2016.

[1635] Blom, 1 Case W. Reserve J.L. Tech. & Internet 36, 58 (2009); Chen/Durkee/Friend/Urban, S. 14 f. (2011); Notice and Takedown in Everday Practice, S. 128.

[1636] Pollack, 22 Santa Clara High Tech. L.J. 547, 574 (2005); Urban/Quilter, 22 Santa Clara Computer & High Tech. L.J. 621, 688 (2006).

[1637] Dies räumen auch Urban/Quilter ein, 22 Santa Clara Computer & High Tech. L.J. 621, 688 f. (2006).

notification auch an den vermeintlichen Rechtsverletzer zu senden.[1638] Dieser Vorschlag verkennt allerdings die Tatsache, dass dem Urheberrechtsinhaber in den meisten Fällen die Identität des vermeintlichen Rechtsverletzers nicht bekannt ist. Dies ist gerade der Grund dafür, dass er nicht den Rechtsverletzer selbst in Anspruch nehmen wird, sondern sich zur Abstellung der Rechtsverletzung des ISP bedient.

c) Unverzügliche Wiederherstellung nach counter notification

Um den Interessen des Inhalteanbieters, welcher einer Urheberrechtsverletzung bezichtigt wird, mehr Gewicht zu verleihen, wird vorgeschlagen, dem ISP die Pflicht aufzuerlegen, das beanstandete Material nach Erhalt einer *counter notification* unverzüglich wieder online zu stellen.[1639] Führt man sich die Tatsache vor Augen, dass der ISP dazu verpflichtet ist, auf die bloße Behauptung hin, das Material *expeditiously* zu entfernen, so ist in der Tat ein Ungleichgewicht zwischen den Interessen der Urheberrechtsinhaber und der Inhalteanbieter nicht von der Hand zu weisen.[1640] Eine Verpflichtung zur unverzüglichen Wiederherstellung des zuvor aufgrund der *notification* entfernten Materials würde die entgegenstehenden Interessen wieder ausbalancieren. Der Rechteinhaber würde hierdurch auch nicht unberechtigt benachteiligt werden, da diesem ja weiterhin die Möglichkeit offen steht, ein Verfahren wegen Urheberrechtsverletzung gegen den vermeintlichen Rechtsverletzer einzuleiten. Eine Pflicht des ISP, bei Klageerhebung das Material wieder zu entfernen bzw. zu sperren, ist nicht zwingend notwendig. Denn zu diesem Zeitpunkt gehen ja beide Parteien, jedenfalls nach ihrer Darlegung im Rahmen der *notification* bzw. *counter notification*, in gutem Glauben davon aus, dass sie im Recht sind. Beide Parteien haben folglich im Rahmen des Verfahrens das

[1638] Chen/Durkee/Friend/Urban, S. 16 (2011).
[1639] Chen/Durkee/Friend/Urban, S. 17 (2011); Pollack, 22 Santa Clara High Tech. L.J. 547, 575 (2005); Urban/Quilter, 22 Santa Clara Computer & High Tech. L.J. 621, 689 (2006); Notice and Takedown in Everday Practice, S. 128.
[1640] So auch Pollack, 22 Santa Clara High Tech. L.J. 547, 561 (2005).

Gericht zunächst davon zu überzeugen, dass eine Urheberrechtsverletzung vorliegt bzw. nicht vorliegt. Es scheint daher gerechtfertigt, in einem solchen Fall, dem ISP keine nochmalige Pflicht zur Entfernung bzw. zur Sperrung des Materials aufzuerlegen.[1641]

d) Verschärfung der Rechtsbehelfe gegen unberechtigte notifications

Zur Stärkung der Interessen der Inhalteanbieter sowie um Urheberrechtsinhaber davon abzuhalten, vorschnell und ohne genauere Prüfung eine *notification* zu versenden, wird weiterhin vorgeschlagen, § 512 (f) DMCA zu modifizieren und den Begriff der *material misrepresentation* durch den der *reckless misrepresentation* zu ersetzen.[1642] Hierdurch würde die hohe Hürde der Geltendmachung von Ansprüchen unter § 512 (f) DMCA interessengerecht gesenkt und ein Anreiz für Urheberrechtsinhaber gesetzt, nicht vorschnell und ohne genaue Prüfung *notifications* zu versenden.[1643] Dies könnte jedoch den Urheberrechtsinhaber in der Geltendmachung seiner Urheberrechte unnötig behindern.[1644]

Weiterhin wird vorgeschlagen, die Sanktionen nach § 512 (f) DMCA zu verschärfen, so dass dieser explizit *punitive* oder *statutory damages* vorsieht.[1645] In der Tat hat der Urheberrechtsinhaber derzeit, auch sofern er absichtlich falsche Angaben in der *notification* vornimmt, nur verhältnismäßig geringe Schadensersatzforderungen zu befürchten. Konkrete Schäden, die von dem Inhalteanbieter erlitten wurden, sind oftmals schwer zu beziffern. Die Einführung spezifischer *statutory damages* würde hier für mehr Klarheit sorgen. Da der Urheberrechtsinhaber zur

[1641] So im Ergebnis auch Pollack, 22 Santa Clara High Tech. L.J. 547, 575 (2005), der ausführt, dass *„[...] content should not be disabled again absent a court order issued after standard court process."*

[1642] Chen/Durkee/Friend/Urban, S. 12 (2011); Notice and Takedown in Everday Practice, S. 128 f. Siehe hierzu auch S. 343.

[1643] Chen/Durkee/Friend/Urban, S. 12 (2011).

[1644] So Rozsnyai, 2 Shidler J. L. Com & Tech. 15 (2006) hinsichtlich der Anlegung eines objektiven Standards zur Bestimmung der *misrepresentation*.

[1645] Für die Einführung von *punitive damages*: Urban/Quilter, 22 Santa Clara Computer & High Tech. L.J. 621, 690 (2006). Für die Einführung von *statutory damages*: Chen/Durkee/Friend/Urban, S. 13 (2011); Notice and Takedown in Everday Practice, S. 129.

Zahlung von *statutory damages* nur verpflichtet werden kann, sofern er willentlich falsche Angaben gemacht hat, sprechen auch keine berechtigten Belange der Urheber gegen eine solche Einführung.

e) Information zur counter notification

Um die Inhalteanbieter in ihren Rechten zu stärken, ist der Vorschlag zu begrüßen, den vermeintlichen Rechtsverletzer im Rahmen der Unterrichtung über eine ihn betreffende *notification* gem. § 512 (g) (2) (A) DMCA über sein Recht zur Einreichung einer *counter notification* sowie weiterer diesbezüglicher Details zu informieren.[1646]

f) Einrichtung eines zentralen Registers

Aufgrund der fehlenden Transparenz des *Notice and Takedown*-Systems wurde der Vorschlag gemacht, ein zentrales öffentliches Register unter Schirmherrschaft des *U.S. Copyright Offices* einzuführen.[1647] Urheberrechtsinhaber sollen entsprechend gesetzlich dazu verpflichtet werden, eine Kopie der an den ISP gesendeten *notification* an das *U.S. Copyright Office* weiterzuleiten.[1648] Erhofft wird sich neben Erkenntnissen über den *Notice and Takedown*-Prozess vor allem eine abschreckende Wirkung hinsichtlich des Missbrauchs dieses Systems durch eine Art *public accountability* (öffentliche Rechenschaftspflicht).

Eine ähnliche Datenbank schlägt *Blom* auch speziell für *notifications* gegenüber *Information Location Tools* vor.[1649]

Es ist jedoch fraglich, ob ein solches öffentliches Register tatsächlich dazu geeignet ist, die Versendung von fehlerhaften oder leichtsinnigen *notifications* zu beeinflussen. Bereits heute leiten viele ISP die von Ihnen empfangenen *notifications* an die Datenbank *Lumen* weiter.[1650] Einen merkbaren Effekt auf die

[1646] So Chen/Durkee/Friend/Urban, S. 16 (2011).
[1647] Chen/Durkee/Friend/Urban, S. 17 f. (2011); Notice and Takedown in Everday Practice, S. 131 f.
[1648] Chen/Durkee/Friend/Urban, S. 16 (2011).
[1649] Blom, 1 Case W. Reserve J.L. Tech. & Internet 36, 57 f. (2009).
[1650] Siehe hierzu S. 392. Hierunter befindet sich auch Google, eine entsprechende

Versendung missbräuchlicher *notifications* scheint dies jedoch nicht zu haben.

IV. Verantwortlichkeit der ISP nach den allgemeinen Gesetzen

Die *safe harbor*-Bestimmungen des DMCA beeinflussen nicht die Verantwortlichkeit der ISP nach den allgemeinen Gesetzen. Sie schränken lediglich die Rechtsfolgen stark ein. Dennoch sind viele Gerichte dazu übergegangen, auf eine (vollständige) Prüfung der Verantwortlichkeit der ISP zu verzichten, sofern eine Anwendbarkeit der *safe harbor*-Bestimmungen abzusehen ist. Entsprechend wurde auch vereinzelt Kritik geübt, dass die *safe harbor*-Bestimmungen des DMCA eine weitere Entwicklung der Rechtsprechung hinsichtlich der zugrundeliegenden Haftung der ISP verhindern würden.[1651]

1. Zivilrechtliche Verantwortlichkeit des Host-Providers

Eine Haftung des Host-Providers kommt theoretisch sowohl als *direct* als auch als *indirect infringer* in Frage. Die Privilegien des § 512 DMCA stehen einer Verantwortlichkeit des Host-Providers nach den allgemeinen Haftungsgrundsätzen nicht entgegen, da sie lediglich die Rechtsfolgen stark einschränken.

a) Direct infringer

Eine Haftung des Host-Providers als *direct infringer* scheidet regelmäßig aufgrund einer fehlenden willentlich rechtsverletzenden Handlungsweise (*volitional infringing conduct*) aus.[1652] Der *Fourth Circuit* vergleicht den Host-Provider mit dem Inhaber eines Kopiergerätes, der dieses der Allgemeinheit zur Nutzung zur Verfügung stellt.[1653] Komme es in diesem Fall zu einer Urheberrechtsverletzung, so sei nicht der Inhaber des Kopiergerätes als *direct infringer* anzusehen, sondern der Nutzer

Info ist abrufbar unter https://support.google.com/legal/answer/1120734, zuletzt besucht am 24.04.2016.
[1651] Walker, Virginia Journal of Law & Technology, Vol. 9, No. 2, para. 27.
[1652] Costar Group, Inc. v. Loopnet, Inc., 373 F.3d 544, 551 (4th Cir. 2004).
[1653] Costar Group, Inc. v. Loopnet, Inc., 373 F.3d 544, 550 (4th Cir. 2004).

des Gerätes.[1654] Genauso verhielt es sich bei dem Host-Provider, dessen System von Dritten zur Verletzung von Urheberrechten genutzt wird und dessen System automatisch das vom Nutzer eingegebene Material hochlädt.[1655] Nach Ansicht des Gerichts verlange der *Copyright Act* einen Willensakt des *direct infringers* sowie einen Kausalzusammenhang, im Gegensatz zu dem passiven Besitz und der Verwaltung eines Internetservices.[1656] Daher scheide eine direkte Haftung für Urheberrechtsverletzungen der Host-Provider aus, sofern das urheberrechtswidrige Material automatisch kopiert, speichert und übermittelt werde.[1657] Liege darüber hinaus eine Beteiligung des Host-Providers vor, so könne dies eine Haftung als *indirect infringer* begründen.[1658]

Zurückzuweisen sind insoweit die Ausführungen des *S.D.N.Y.* in *Arista Records v. Usenet.com*, dass der Host-Provider aufgrund seiner aktiven Beteiligung an Urheberrechtsverletzungen als *direct infringer* hafte.[1659] Das Gericht begründete dies zum einen damit, dass der Host-Provider eigens einen Server für Musikdateien errichtete und aktive Schritte unternehme, wie bspw. das automatische Filtern und die manuelle Überprüfung von Inhalten, um den Zugang zu bestimmten Inhalten sowie bestimmte Nutzer zu sperren.[1660] Der Host-Provider hätte somit auch Kontrolle über die Inhalte seiner Nutzer.[1661] Er gehe damit über eine passive Funktion hinaus und erfülle die für den *direct infringer* vorausgesetzte willentliche Handlung.[1662] Entgegen der Auffassung des Gerichts wird durch diese Handlungen des Host-Providers jedoch keine

---

[1654] Costar Group, Inc. v. Loopnet, Inc., 373 F.3d 544, 550 (4th Cir. 2004).
[1655] Costar Group, Inc. v. Loopnet, Inc., 373 F.3d 544, 550 (4th Cir. 2004).
[1656] Costar Group, Inc. v. Loopnet, Inc., 373 F.3d 544, 550 (4th Cir. 2004).
[1657] Costar Group, Inc. v. Loopnet, Inc., 373 F.3d 544, 555 (4th Cir. 2004); *„[...] we hold that the automatic copying, storing, and transmission of copyrighted materials, when instigated by others, does not render the ISP strictly liable for copyright infringement under §§ 501 and 106 of the Copyright Act."*
[1658] Costar Group, Inc. v. Loopnet, Inc., 373 F.3d 544, 555 (4th Cir. 2004).
[1659] Arista Records LLC v. Usenet.com, 633 F. Supp. 2d 124, 149 (S.D.N.Y. 2009).
[1660] Arista Records LLC v. Usenet.com, 633 F. Supp. 2d 124, 148 (S.D.N.Y. 2009).
[1661] Arista Records LLC v. Usenet.com, 633 F. Supp. 2d 124, 148 ff. (S.D.N.Y. 2009).
[1662] Arista Records LLC v. Usenet.com, 633 F. Supp. 2d 124, 149 (S.D.N.Y. 2009).

direkte Urheberrechtsverletzung begründet, sondern diese können vielmehr eine indirekte Haftung nach den bekannten Instrumenten der *secondary liability* auslösen. So ist beispielsweise die von dem *S.D.N.Y.* angesprochene Kontrolle ein Merkmal der *vicarious liability*. Zudem erscheint es höchst fragwürdig, durch freiwillige Überwaschungs- und Filterungsmaßnahmen des Host-Providers überhaupt eine Haftung zu kreieren. Die Entscheidungsgründe des *S.D.N.Y.* hinsichtlich der *direct liability* des Host-Providers sind folglich abzulehnen.[1663] Vielmehr ist darauf abzustellen, wer tatsächlich die rechtsverletzende Handlung begangen hat.[1664]

b) Indirect infringer

Der Host-Provider könnte jedoch als *indirect infringer* für Urheberrechtsverletzungen seiner Nutzer haften.

aa) Contributory liability

Denkbar wäre zunächst eine Haftung als *contributory infringer*. Dazu müsste der Host-Provider Kenntnis von der Rechtsverletzung im Sinne einer tatsächlichen Kenntnis oder Kennenmüssen haben sowie maßgeblich zu der Rechtsverletzung beigetragen haben. Bereits der *N.D. California* hat 1995 in dem „Netcom"-Fall entschieden, dass die Mitteilung einer Rechtsverletzung an einen Access-Provider dessen Kenntnis begründen kann.[1665] Auch der *S.D.N.Y.* hat eine *contributory liability* in einem Fall bejaht, in dem der Host-Provider durch eine *notification* über Rechtsverletzungen benachrichtigt wurde, es allerdings unterlassen hat, das Material zu entfernen bzw. zu sperren.[1666] Die Kenntnis wurde in diesem Fall durch die gesendeten *notifications* begründet, der maßgebliche

[1663] So auch Perfect 10, Inc. v. Giganews, Inc., 2014 U.S. Dist. LEXIS 183592 (C.D. Cal. 2014) at *28.
[1664] Perfect 10, Inc. v. Giganews, Inc., 2014 U.S. Dist. LEXIS 183592 (C.D. Cal. 2014) at *28.
[1665] Religious Technology Center v. Netcom On-Line Communication Services, Inc., 907 F.Supp. 1361, 1374 et seqq. (1995).
[1666] Capitol Records, Inc., v. MP3Tunes, LLC, 821 F.Supp.2d 627, 649 (S.D.N.Y. 2011).

Beitrag bestand darin, dass der Host-Provider den Service zur Begehung der Urheberrechtsverletzungen zur Verfügung stellte.[1667]

bb) Vicarious liability

Zudem ist eine Haftung aus *vicarious infringement* denkbar. In *Netcom* sah der *N.D. California* das Recht und die Möglichkeit einer Kontrolle durch den Host-Provider darin, dass dieser in mehreren Fällen Nutzer von der Nutzung seines Dienstes ausschloss sowie die Möglichkeit besaß, Inhalte zu löschen.[1668] Das notwendige zweite Merkmal der *vicarious liability*, der direkte finanzielle Vorteil, verneinte das Gericht allerdings, da der Host-Provider eine pauschale Vergütung von seinen Nutzern erhielt und es keine Anhaltspunkte dafür gab, dass rechtsverletzende Inhalte den Wert des Services steigerten oder neue Nutzer anlockten.[1669]

cc) Inducement liability

Der Host-Provider könnte auch nach den Grundsätzen der *inducement liability* haften. In *Columbia v. Fung* bejahte der *Ninth Circuit* eine entsprechende Haftung des Host-Providers aufgrund der Zurverfügungstellung eines Services sowie der anschließenden Förderung von Urheberrechtsverletzungen durch eigene Maßnahmen.[1670] Der Host-Provider hatte seine Nutzer ermutigt, Dateien mit urheberrechtlich geschütztem Inhalt hochzuladen, beispielsweise durch Bereitstellung einer Liste der 20 umsatzstärksten Kinofilme auf seiner Webseite. Sofern ein Nutzer einzelne Filme dieser Liste anklickte, wurde er gebeten eine Datei des Films hochzuladen.[1671] Der Host-Provider war Nutzern zudem bei dem Upload und bei der Lokalisierung von urheberrechtlich geschützten Werken behilflich und berat die Nutzer

[1667] Capitol Records, Inc., v. MP3Tunes, LLC, 821 F.Supp.2d 627, 648 (S.D.N.Y. 2011).
[1668] Religious Technology Center v. Netcom On-Line Communication Services, Inc., 907 F.Supp. 1361, 1376 (1995).
[1669] Religious Technology Center v. Netcom On-Line Communication Services, Inc., 907 F.Supp. 1361, 1377 (1995).
[1670] Columbia Pictures Industries, Inc. v. Fung, 710 F.3d 1020, 1033 ff. (9th Cir. 2013).
[1671] Columbia Pictures Industries, Inc. v. Fung, 710 F.3d 1020, 1036 (9th Cir. 2013).

diesbezüglich.[1672] Des Weiteren postete der Host-Provider Nachrichten innerhalb des Forums, in denen er Nutzer bat, spezifische urheberrechtlich geschützte Filme hochzuladen.[1673] Dass der Host-Provider eine entsprechende Absicht zur Förderung von Rechtsverletzungen hatte, schloss der *Ninth Circuit* zudem aus der Tatsache, dass der Host-Provider seinen Umsatz fast ausschließlich durch den Verkauf von Werbeflächen generierte und die Einnahmen entsprechend abhängig von den Nutzerzahlen waren.[1674] Hinsichtlich des Erfordernisses der Kausalität führt der *Ninth Circuit* aus, dass derjenige, der einen Service zur Verfügung stellt, mit dem Urheberrechtsverletzungen begangen werden können mit der offensichtlichen Absicht, dass der Service auch dafür genutzt wird, auch kausal verantwortlich für die über seinen Service begangenen Urheberrechtsverletzungen ist.[1675]

2. Strafrechtliche Verantwortlichkeit des Host-Providers

Die strafrechtliche Verantwortlichkeit für Urheberrechtsverletzungen ist in 17 U.S.C. § 506 geregelt. Dieser bestimmt, dass jede Person, die vorsätzlich das Urheberrecht verletzt gem. 18 U.S.C. § 2319 bestraft wird, sofern (1) die Rechtsverletzung entweder für Zwecke des wirtschaftlichen Vorteils oder privaten finanziellen Bereicherung[1676], (2) die während eines Zeitraums von 180 Tagen vervielfältigten oder verbreiteten Kopien einen Handelswert von über $ 1.000 haben[1677] oder (3) ein Urheberrechtswerk, welches gerade für den kommerziellen Vertrieb vorbereitet wird, durch ein Computernetzwerk den Mitgliedern der Öffentlichkeit zugänglich gemacht wird, sofern diese Person wusste oder hätte wissen

[1672] Columbia Pictures Industries, Inc. v. Fung, 710 F.3d 1020, 1036 (9th Cir. 2013).
[1673] Columbia Pictures Industries, Inc. v. Fung, 710 F.3d 1020, 1037 (9th Cir. 2013).
[1674] Columbia Pictures Industries, Inc. v. Fung, 710 F.3d 1020, 1036 (9th Cir. 2013).
[1675] Columbia Pictures Industries, Inc. v. Fung, 710 F.3d 1020, 1037 (9th Cir. 2013).
[1676] 17 U.S.C. § 506 (1) (A).
[1677] 17 U.S.C. § 506 (1) (B).

müssen, dass das Werk für den kommerziellen Vertrieb vorbereitet wird[1678]. Kurz gefasst erfordert die strafrechtliche Haftung demnach drei Elemente: Eine Urheberrechtsverletzung, die vorsätzlich und mit dem Zweck des wirtschaftlichen Vorteils bzw. der privaten finanziellen Bereicherung begangen wurde. Hinsichtlich des Vorsatzes bestimmt 17 U.S.C. § 506 (a) (2), dass Beweise einer Vervielfältigung bzw. Verbreitung eines Urheberrechtswerkes alleine nicht ausreichend sind, um Vorsatz zu begründen. Um Vorsatz nachzuweisen ist vielmehr zunächst eine Kenntnis der Rechtsverletzung erforderlich und zudem müssen sie absichtlich eine bekannte Pflicht verletzt haben.[1679] Damit ist ein unwissender Verletzer, der zwar absichtlich eine bestimmte Handlung vornimmt, aber in dem aufrichtigen Glauben, dass diese rechtmäßig ist, nicht als *willfully infringer* anzusehen.[1680]

Die Folgen einer strafrechtlichen Verantwortlichkeit nach 17 U.S.C. § 506 reichen von 1 bis 10 Jahren Haft[1681] sowie einer Geldstrafe bis zu $ 250.000[1682]. Die genaue Höhe der Haft- oder Geldstrafe ist zum einen abhängig von dem jeweils einschlägigen Delikt des 17 U.S.C. § 506, zum anderen von der jeweiligen Schwere der konkreten Rechtsverletzung.

Der wohl bislang bekannteste Fall eines Vorgehens wegen strafrechtlicher Urheberrechtsverletzung gegen einen Host-Provider ist der Fall Megaupload.[1683] Das *U.S. Department of Justice* erhob hier Anklage u.a. wegen strafrechtlicher Urheberrechtsverletzungen. Die Anklage erfuhr erhebliche Kritik, insbesondere da sie die strafrechtliche Verfolgung auf einen Bereich erstreckt, der ursprünglich als zivilrechtliche Verletzungshandlung klassifiziert wurde.[1684] Insbesondere kritisiert

---

[1678] 17 U.S.C. § 506 (1) (C).

[1679] Nimmer on Copyright, § 15.01 [A] [2]: *„[...] 'willfulness' required for criminal copyright infringement as a 'voluntary, intentional violation of a known legal duty'."*

[1680] Martin/Newhall, 15 N.C. J. L. & Tech. 101, 128 (2013).

[1681] 18 U.S.C. § 2319.

[1682] 18 U.S.C. § 3571.

[1683] United States of America v. Kim Dotcom, 212 U.S. Dist. LEXIS 148114 (E.D. Va., Oct. 5, 2012).

[1684] Blevins, 34 Cardozo L. Rev. 1821, 1868 (2013); Corwin, MegaBust's

wird, dass die Anklageschrift sich hauptsächlich auf Verletzungshandlungen im Bereich der *secondary liability* bezieht, vornehmlich auf die sogenannte *inducement liability*, welche dem *common law* Bereich entstammt und somit nicht die Basis für eine strafrechtliche Verantwortlichkeit sein könne.[1685] Zudem sei es zu bezweifeln, ob hier eine vorsätzliche Rechtsverletzung durch Megaupload vorliege.[1686] Sofern vereinzelt Stimmen davon ausgehen, dass Fälle von *aiding and abetting* im Bereich des Urheberstrafrechts nicht anerkannt sind[1687], ist dies abzulehnen.[1688] Gerade die gesetzliche Festschreibung in § 2 des U.S.C. Title 18 „Crimes and Criminal Procedure", dass derjenige als Täter zu qualifizieren ist, der die Rechtsverletzung unterstützt, begünstigt, befehlt oder sonst wie veranlasst (kurz: *aiding and abetting*)[1689], kann vielmehr dahingehend ausgelegt werden, dass eine Verantwortlichkeit im Sinne der zivilrechtlichen *common law secondary liability* zur strafrechtlichen Verfolgung erst gar nicht gegeben sein muss.[1690] Entsprechend wird teilweise die durch das *common law* entwickelte *secondary liability* auch als Gegenstück zum strafrechtlichen *aiding and abetting* angesehen.[1691] Unklar sind allerdings die genauen Konturen des *aiding and abedding im* Bereich des Urheberrechts. Insbesondere ist fraglich, ob zu deren

---

MegaQuestions Cloud the Net's Future; Granick, Megaupload: A lot less guilty than you think; Falzone/Granick, Megaupload.com indictment leaves everyone guessing – Part 1; Lessig, Expert Opinion, S. 12.

[1685] Blevins, 34 Cardozo L. Rev. 1821, 1868 (2013); Megaupload: A lot less guilty than you think.

[1686] Blevins, 34 Cardozo L. Rev. 1821, 1869 (2013).

[1687] So bspw. Manta, 24 Harv. J.L. & Tech. 469, 481 (2011); Lessig, Expert Opinion, S. 13.

[1688] Martin/Newhall, 15 N.C. J. L. & Tech. 101, 108 (2013); Siehe auch Sydnor, der darauf hinweist, dass der Grund dafür, dass der Copyright Act 1976 die explizite Nennung des *aiding and abetting* aus § 506 entfernt hat (welche in dem 1909 Copyright Act noch enthalten war), lediglich darauf zurückzuführen ist, dass zwischenzeitlich eine entsprechende Klausel bzgl. *aiding and abetting* in 18 U.S.C. § 2 aufgenommen wurde und somit unnötige Wiederholungen vermieden werden sollten.

[1689] 18 U.S.C. § 2 (a): *„Whoever commits an offense against the United States or aids, abets, counsels, commands, induces or procures its commission, is punishable as a principal."*

[1690] So auch Martin/Newhall, 15 N.C. J. L. & Tech. 101, 121 (2013).

[1691] In re Aimster Copyright Litigation, 334 F.3d 643, 651 (2003); Martin/Newhall, 15 N.C. J. L. & Tech. 101, 121 (2013); Charlesworth, Stan. Tech. L. Rev. 6, 44 (2011).

Bestimmung die aus dem Bereich des Zivilrechts im Rahmen der *secondary liability* entwickelten Maßstäbe herangezogen werden können.

Martin und *Newhall* plädieren dafür, dass beide Konzepte dieselben Handlungen erfassen.[1692] Es sei daher für eine strafrechtliche Verfolgung ausreichend, wenn eine Haftung als *secondary infringer* gegeben sei.[1693] Dem ist nicht zuzustimmen. Es mag Fälle geben, in denen die Handlung des Host-Providers diesen als indirekten Rechtsverletzer nach der *secondary liability* haften lässt und diese Handlung zugleich auch als Fall des *aiding and abetting* im strafrechtlichen Sinne klassifiziert werden kann. Oftmals wird allerdings die Handlung des Host-Providers nicht als vorsätzliche Handlung im strafrechtlichen Sinne angesehen werden können, so dass zwar eine zivilrechtliche *secondary liability* gegeben ist, aber kein strafrechtliches *aiding and abetting*.

Der Fall Megaupload ist, obwohl die Anklage bereits aus 2012 stammt, noch immer nicht entschieden, da sich die Angeklagten in Neuseeland befinden, wo derzeit noch ein Verfahren bzgl. der Auslieferung an die USA anhängig ist.

Die Frage, ob ein Host-Provider, der nicht als direkter Rechtsverletzer klassifiziert werden kann, überhaupt strafrechtlich für Urheberrechtsverletzungen haftbar gemacht werden kann, ist damit noch immer gerichtlich nicht entschieden worden.

3. Zivilrechtliche Verantwortlichkeit des Cache-Providers

Eine Haftung des Cache-Providers wurde bislang von der Rechtsprechung noch nicht explizit behandelt. Allerdings lassen sich die Grundsätze eines frühen Urteils, welches vor der Umsetzung des DMCA im Hinblick auf den Access-Provider ergangen ist, auf den Cache-Provider übertragen. In *Religious Technology Center v. Netcom* wurde die Verantwortlichkeit eines ISP, welcher Zugang zu einem Usenet herstellte und in diesem Zusammenhang das Material im Rahmen der Übermittlung für 11

[1692] Martin/Newhall, 15 N.C. J. L. & Tech. 101, 121 (2013).
[1693] Martin/Newhall, 15 N.C. J. L. & Tech. 101, 140 (2013).

Tage zwischenspeicherte, analysiert.[1694] Die Speicherung geschah laut Sachverhaltsdarstellung zur Erleichterung der Übermittlung und zum Komfort der Usenet-Nutzer.[1695] Zur Beurteilung dieser Tätigkeit ist es erforderlich, sich nochmals die Tätigkeitsbereiche des Access-Providers und des Cache-Providers anzuschauen und diese insbesondere im Hinblick auf das Merkmal der zwischenzeitlichen Speicherung abzugrenzen. Der bloße Gesetzeswortlaut ist hier keine große Hilfe. Zwar spricht § 512 (a) DMCA bei dem Access-Provider von einer *„intermediate and transient storage“* während § 512 (b) von *„intermediate and temporary storage“* spricht, eine genaue Abgrenzung kann aufgrund dieses unterschiedlichen Wortlauts allerdings nicht vorgenommen werden, da beide Begriffe nicht scharf umrissen sind. Eine klare Abgrenzung kann vielmehr im Hinblick auf den Zweck der Zwischenspeicherung vorgenommen werden. So dient die Zwischenspeicherung des Access-Providers lediglich dazu, das Material von Nutzer A zu Nutzer B zu übertragen, während die Zwischenspeicherung des Cache-Providers dazu dient, das Material welches ursprünglich von Nutzer A zu Nutzer B übertragen wurde, weiteren Nutzern schnell und effizient zur Verfügung zu stellen. Führt man sich diesen Sinn und Zweck der Zwischenspeicherung vor Augen, so liegt die Vermutung nahe, dass die Tätigkeit von Netcom im streitgegenständlichen Fall, eher der eines Cache-Providers entspricht.

Die in dem Urteil aufgeführten Maßstäbe können deshalb für die Bewertung der Verantwortlichkeit des Cache-Providers herangezogen werden.

a) Direct Infringer

Eine Haftung des Cache-Providers als direkter Rechtsverletzer dürfte grundsätzlich nicht bestehen. Da der Cache-Provider

[1694] Religious Technology Center v. Netcom On-line Communication Services, Inc., 907 F.Supp. 1361, 1367 (N.D.Cal. 1995).

[1695] Religious Technology Center v. Netcom On-line Communication Services, Inc., 907 F.Supp. 1361 (N.D.Cal. 1995):*„In order to ease transmission and for the convenience of Usenet users, Usenet servers maintain postings from newsgroups for a short period of time – eleven days for Netcom's system [...]“*.

lediglich Nutzeranfragen durch sein System automatisch ausführt, fehlt es bereits an einer wie auch immer gearteten willentlichen Handlung des Cache-Providers.[1696] Einen solchen Provider als direkten Rechtsverletzer verantwortlich zu machen würde zur Haftung unzähliger Beteiligter führen, deren Rolle in nicht mehr besteht, als ein System zu errichten und zu betreiben, welches für das Funktionieren des Internets von großem Vorteil ist.[1697]

b) Indirect Infringer

Denkbar wäre hingegen eine Haftung des Cache-Providers als *indirect infringer*.

aa) Contributory Infringement

Für die Haftung als *contributory infringer* wird die Kenntnis einer Urheberrechtsverletzung sowie ein maßgeblicher Beitrag hierzu vorausgesetzt. In *Netcom* hat der *N.C. California* ausgeführt, dass eine Kenntnis zu dem Zeitpunkt vorliegen könnte als der Provider von dem Urheberrechtsinhaber über die rechtsverletzenden Aktivitäten des Usenet-Nutzers in Kenntnis gesetzt wurde.[1698]

Der wesentliche Beitrag zur Urheberrechtsverletzung könne darin liegen, dass durch die Zurverfügungstellung des Services automatisch alle Beiträge des Usenets verbreitet werden.[1699] Der Provider ermögliche dem rechtsverletzenden Usenet-Nutzer, dass dessen rechtsverletzendes Material auf dem System des Providers verweile und dadurch an weitere Usenet Server weltweit verbreitet werde.[1700]

[1696] Religious Technology Center v. Netcom On-line Communication Services, Inc., 907 F.Supp. 1361, 1370 (N.D.Cal. 1995).
[1697] Religious Technology Center v. Netcom On-line Communication Services, Inc., 907 F.Supp. 1361, 1372 (N.D.Cal. 1995).
[1698] Religious Technology Center v. Netcom On-line Communication Services, Inc., 907 F.Supp. 1361, 1372 (N.D.Cal. 1995).
[1699] Religious Technology Center v. Netcom On-line Communication Services, Inc., 907 F.Supp. 1361, 1375 (N.D.Cal. 1995).
[1700] Religious Technology Center v. Netcom On-line Communication Services, Inc., 907 F.Supp. 1361, 1375 (N.D.Cal. 1995).

Der Provider sei in der Lage einfache Schritte zu unternehmen um weiteren Schaden hinsichtlich des urheberrechtlichen Werkes zu vermeiden.[1701]

Demnach ist eine Haftung des Cache-Providers als *indirect infringer* in Fällen denkbar, in denen der Cache-Provider auf eine Urheberrechtsverletzung hingewiesen wurde, es aber dennoch versäumt, entsprechende Schritte zur Entfernung des Materials aus seinem Zwischenspeicher zu unternehmen.

bb) Vicarious infringement

Eine Haftung als *vicarious infringer* setzt voraus, dass der Cache-Provider das Recht und die Möglichkeit hat, die rechtsverletzende Aktivität zu überwachen sowie einen finanziellen Vorteil hieraus zieht. Während nach Ansicht des *N.D. California* in *Netcom* das erste Merkmal gegeben sei, da der Provider die Möglichkeit habe bestimmte Materialien, die er zwischenspeichert, zu löschen oder bestimmte Nutzer komplett zu blockieren, liege ein finanzieller Vorteil des Providers aus der rechtsverletzenden Tätigkeit nicht vor.[1702] Der Provider erhob eine Fixgebühr für seinen Service, es gab keine Anzeichen dafür, dass die Rechtsverletzungen durch die Nutzer des Usenets die Attraktivität des Services steigern würden.[1703]

Entsprechend wird eine Haftung des Cache-Providers aus *vicarious infringement* regelmäßig nicht gegeben sein.

cc) Inducement liability

Eine Haftung im Sinne der *inducement liability* ist denkbar, sofern der Cache-Provider seinen Service mit dem Ziel betreibt, Urheberrechtsverletzungen zu fördern. Der Cache-Provider übermittelt Inhalte, die sich auf anderen Newsservern befinden an seine Nutzer und speichert diese in diesem Zusammenhang

[1701] Religious Technology Center v. Netcom On-line Communication Services, Inc., 907 F.Supp. 1361, 1375 (N.D.Cal. 1995).
[1702] Religious Technology Center v. Netcom On-line Communication Services, Inc., 907 F.Supp. 1361, 1376 (N.D.Cal. 1995).
[1703] Religious Technology Center v. Netcom On-line Communication Services, Inc., 907 F.Supp. 1361, 1377 (N.D.Cal. 1995).

kurzzeitig zwischen. Eine Förderung von Rechtsverletzungen, also entweder dem Hochladen von urheberrechtlich geschützten Dateien durch die Nutzer des anderen Newsservers oder aber das Downloaden von urheberrechtlich geschützten Dateien durch seine eigenen Nutzer ist eher unwahrscheinlich. Die Nutzer des anderen Newsservers liegen schon nicht in der unmittelbaren Einfluss-Sphäre des Cache-Providers. Theoretisch denkbar, aber praktisch unwahrscheinlich ist eine Förderung von Rechtsverletzungen durch seine Nutzer, beispielsweise durch explizite Bewerbung urheberrechtsverletzender Downloads. Hierfür müsste der Cache-Provider allerdings Kenntnis über bestimmte urheberrechtsverletzende Inhalte auf den anderen Newsservern haben, die seine Nutzer anfordern können. Eine *inducement liability* des Cache-Providers ist daher unwahrscheinlich.

4. Strafrechtliche Haftung des Cache-Providers

Eine strafrechtliche Verantwortlichkeit des Cache-Providers würde eine vorsätzliche Urheberrechtsverletzung, welche auf den wirtschaftlichen Vorteil bzw. die private finanzielle Bereicherung ausgelegt ist, voraussetzen. Strafrechtliche Verfahren gegen Cache-Provider sind bislang nicht bekannt und auch hinsichtlich der üblicherweise neutralen und automatisierten Tätigkeit eher unwahrscheinlich. Um strafrechtlich belangt zu werden, müsste der Cache-Provider vorsätzlich selbst oder mit Hilfe eines anderen, bspw. dem Nutzer des Usenet-Services, mit Wissen und Wollen eine Urheberrechtsverletzung begehen.

5. Zivilrechtliche Verantwortlichkeit des Access-Providers

Eine Haftung des Access-Providers kommt theoretisch sowohl als direkter als auch als indirekter Rechtsverletzer in Frage. Der Fall Netcom kann hier als wegweisend angesehen werden. Bei der Anwendung der vom *N.D. California* aufgestellten Grundsätze auf den Access-Provider ist allerdings Vorsicht geboten. Auch wenn das Gericht in diesem frühen Urteil von einem Access-Provider spricht, so ist zu bezweifeln, dass eine entsprechende

Klassifizierung auch noch heute Bestand hätte. Vielmehr scheint es, dass die mittlerweile auch im DCMA festgeschriebene Tätigkeit des Cache-Providers hier einschlägig ist. Der typische Access-Provider wird Material nur lediglich in dem Umfang kurzzeitig zwischenspeichern wie dies für die reine Übermittlung bzw. Zugangsvermittlung notwendig ist. Eine Dauer von 11 Tagen wird hier nicht mehr als notwendig für den reinen Übermittlungsvorgang angesehen werden können.

a) Direct infringer

Eine Haftung des Access-Providers als direkter Verletzer scheidet regelmäßig aus. Der *N.D. California* hat in dem „Netcom"-Fall entschieden, dass der Access-Provider, der Kopien von Material, welches im Usenet hochgeladen wird, automatisch während des Übermittlungsvorgangs kurzzeitig zwischenspeichert, nicht als direkter Verletzer angesehen werden kann.[1704] Da hier der ursprüngliche Usenet-Benutzer das rechtsverletzende Material direkt durch seinen Upload verletzt hat, mache es keinen Sinn, den Access-Provider, dessen System lediglich Nutzeranfragen automatisch ausführt, zusätzlich als direkten Verletzer anzusehen.[1705] Auch wenn die im Netcom-Fall behandelte Tätigkeit, wie zuvor ausgeführt, eher der eines Cache-Providers als der eines Access-Providers entsprach, kann diese Argumentation ohne Weiteres auf den Access-Provider übertragen werden. Der Access-Provider übermittelt Material lediglich automatisch auf Nutzeranfrage, welches ggf. in diesem Zusammenhang lediglich kurzzeitig zwischengespeichert wird.

Eine Klassifizierung des Access-Providers als direkter Rechtsverletzer im Rahmen einer zivilrechtlichen Verantwortlichkeit ist daher grundsätzlich abzulehnen.[1706]

[1704] Religious Technology Center v. Netcom On-line Communication Services, Inc., 907 F.Supp. 1361, 1372 (N.D.Cal. 1995).
[1705] Religious Technology Center v. Netcom On-line Communication Services, Inc., 907 F.Supp. 1361, 1372 (N.D.Cal. 1995).
[1706] So auch Kopko, 8 Computer L. Rev. & Tech. J. 83, 100 f. (2003).

b) Indirect infringer

Der Access-Provider könnte jedoch aus der *secondary liability* als indirekter Rechtsverletzer haften.

aa) Contributory liability

Denkbar wäre zunächst eine Haftung wegen *contributory infringement*. Hierfür notwendig ist eine Kenntnis des Access-Providers sowie ein maßgeblicher Beitrag zur Rechtsverletzung. Der *N.C. California* hat in seinem „Netcom"-Fall hinsichtlich der Kenntnis ausgeführt, dass maßgeblich auf den Zeitpunkt abgestellt werden könne, an dem der Access-Provider von dem Urheberrechtsinhaber über die rechtsverletzenden Aktivitäten des Usenet-Nutzers benachrichtigt wurde.[1707]

Es ist fraglich, ob diese Argumentation auch auf den Access-Provider passt. Bei diesem dürfte es in der Regel an der notwendigen Kenntnis der Rechtsverletzung fehlen. Denn selbst wenn der Access-Provider von dem Urheber bzgl. der Übermittlung von rechtsverletzendem Material in Kenntnis gesetzt wird, so wird der Übermittlungsvorgang bereits abgeschlossen sein, so dass eine Handhabe des Access-Providers in dem konkreten Fall ohnehin ausgeschlossen ist. Eine Kenntnis liegt zu dem Zeitpunkt der Rechtsverletzung daher nicht vor. Anders kann dies lediglich bei der Tätigkeit der Zugangsvermittlung beurteilt werden. Wurde der Access-Provider darüber in Kenntnis gesetzt, dass sich auf einer bestimmten Seite, zu der er Zugang vermittelt, urheberrechtsverletzendes Material befindet und stellt er weiterhin den Zugang zu diesem Material her, so könnte dies eine Kenntnis im Sinne der *contributory liability* begründen.

Hinsichtlich des notwendigen wesentlichen Beitrags durch den Access-Provider führte das Gericht aus, dass die Zurverfügungstellung eines Services durch den automatisch alle Beiträge des Usenets verbreitet werden, weit über das reine Vermieten von Räumlichkeiten an einen Rechtsverletzer

[1707] Religious Technology Center v. Netcom On-line Communication Services, Inc., 907 F.Supp. 1361, 1374 (N.D.Cal. 1995).

hinausgehe.[1708] Der Access-Provider ermögliche dem rechtsverletzenden Usenet-Nutzer, dass dessen rechtsverletzendes Material auf dem System des Access-Providers verweile und dadurch an weitere Usenet Server weltweit verbreitet werde.[1709]

Daher sei es angemessen anzunehmen, dass der Access-Provider in der Lage ist, einfache Schritte zu unternehmen, um weiteren Schaden hinsichtlich des urheberrechtlichen Werkes zu vermeiden.[1710] Eine Verantwortlichkeit aufgrund *contributory infringement* sei daher denkbar.[1711]

Auch diese Argumentation des Gerichts kann nicht ohne Weiteres auf den Access-Provider übertragen werden.

Es ist bislang ungeklärt, ob die übliche Tätigkeit des Access-Providers eine solche *material contribution* darstellen kann.[1712] Im Gegensatz zu einem Host-Provider, wo bereits die Zurverfügungstellung der *site and facilities* als ausreichend erachtet wird, stellt der Access-Provider lediglich einen Service zur Übermittlung bzw. zur Zugangsverschaffung zur Verfügung. Es ist fraglich, ob dies bereits als ausreichend erachtet werden kann.[1713] In einer entsprechend weiten Auslegung der bislang aufgestellten Grundsätze einer *contributory liability* wäre es nicht auszuschließen, dass ein Gericht den Access-Provider als *contributory infringer* einstufen könnte.[1714] Eine Haftung wäre daher grundsätzlich denkbar. Allerdings unterscheidet sich die klassische Tätigkeit des Access-Providers erkennbar von den bisher behandelten Fällen, wie bspw. dem Betreiber eines Flohmarktes oder auch dem alleinigen Zugangsanbieter zum Usenet.[1715] Vor diesem Hintergrund könnte ein Gericht zu dem Ergebnis gelangen,

---

[1708] Religious Technology Center v. Netcom On-line Communication Services, Inc., 907 F.Supp. 1361, 1375 (N.D.Cal. 1995).
[1709] Religious Technology Center v. Netcom On-line Communication Services, Inc., 907 F.Supp. 1361, 1375 (N.D.Cal. 1995).
[1710] Religious Technology Center v. Netcom On-line Communication Services, Inc., 907 F.Supp. 1361, 1375 (N.D.Cal. 1995).
[1711] Religious Technology Center v. Netcom On-line Communication Services, Inc., 907 F.Supp. 1361, 1375 (N.D.Cal. 1995).
[1712] Kopko, 8 Computer L. Rev. & Tech. J. 83, 85 (2003).
[1713] So auch Kopko, 8 Computer L. Rev. & Tech. J. 83, 108 (2003).
[1714] So auch Kopko, 8 Computer L. Rev. & Tech. J. 83, 106 (2003).
[1715] So auch Kopko, 8 Computer L. Rev. & Tech. J. 83, 107 f. (2003).

dass selbst eine Auslegung der bisherigen Grundsätze im weitesten Sinne, keine *material contribution* des Access-Providers rechtfertigt.[1716]

bb) Vicarious liability

Auch die Frage der *vicarious liability* wurde in der „Netcom"-Entscheidung beleuchtet. Das Gericht führte aus, dass die Tatsache, dass der Access-Provider entweder die Möglichkeit habe bestimmte Materialien, die er zwischenspeichert, zu löschen oder aber bestimmte Nutzer komplett zu blockieren, dafür ausreiche, das Merkmal der *right and ability to control* zu bejahen.[1717] Eine Haftung als *vicarious infringer* scheiterte aber letzten Endes daran, dass der Access-Provider keinen direkten finanziellen Vorteil aus der Rechtsverletzung zog.[1718] Der Access-Provider erhob eine Fixgebühr, es lag keine Vermutung dafür vor, dass die Rechtsverletzungen durch Nutzer des Usenets die Attraktivität des Services des Access-Providers steigern würden.[1719]

Diese Beurteilungsmaßstäbe gelten grundsätzlich auch für die klassische Tätigkeit des Access-Providers, mit dem Unterschied, dass es im Rahmen einer einfachen Übermittlungstätigkeit zudem an einer *right and ability to control* fehlen dürfte.

Eine Haftung aufgrund der *vicarious liability* ist daher grundsätzlich zu verneinen.[1720]

cc) Inducement liability

Damit den Access-Provider eine *inducement liability* trifft, müsste er die Absicht haben, mit der Zurverfügungstellung seines Dienstes, Rechtsverletzungen zu fördern. Der Access-Provider stellt im Regelfall lediglich die technische Infrastruktur zur Verfügung. Es ist äußerst unwahrscheinlich, dass er seinen Dienst

[1716] So auch Kopko, 8 Computer L. Rev. & Tech. J. 83, 108 (2003).
[1717] Religious Technology Center v. Netcom On-line Communication Services, Inc., 907 F.Supp. 1361, 1376 (N.D.Cal. 1995).
[1718] Religious Technology Center v. Netcom On-line Communication Services, Inc., 907 F.Supp. 1361, 1377 (N.D.Cal. 1995).
[1719] Religious Technology Center v. Netcom On-line Communication Services, Inc., 907 F.Supp. 1361, 1377 (N.D.Cal. 1995).
[1720] So auch Kopko, 8 Computer L. Rev. & Tech. J. 83, 103 (2003).

betreibt, mit der Absicht der Förderung von Urheberrechtsverletzungen. Es ist bereits nicht ersichtlich, welchen Vorteil dies für den Access-Provider bringen würde.
In der Regel wird daher eine *inducement liability* des Access-Providers nicht gegeben sein.

c) Zivilrechtliche Verantwortlichkeit des WLAN-Anbieters

Fraglich ist, ob den Anbieter eines offenen WLAN eine zivilrechtliche Haftung trifft. Bislang wurde dies noch von keinem Gericht entschieden.[1721]
Rechteinhaber haben in diesem Zusammenhang vereinzelt versucht, den Inhaber des WLAN-Anschlusses unter einer *state claim*[1722] der sog. *theory of negligence*[1723] zur Verantwortung zu ziehen.[1724] Hierbei wurde eine Analogie zum Waffeninhaber, der seine geladene Waffe in Reichweite eines Kindes liegen ließ oder einem Autoinhaber, der seine Schlüssel im offenen Auto liegen lies, gezogen.[1725] In einigen Bundesstaaten folgt hieraus eine Verantwortlichkeit wegen fahrlässigem Handeln.[1726]
Eine entsprechende Klage wegen Fahrlässigkeit hinsichtlich eines nicht verschlüsselten privaten WLAN-Anschlusses lag auch dem *S.D.N.Y.* vor.[1727] Das Gericht lehnte einen Anspruch aus bundesstaatlichem Recht aufgrund 17 U.S.C. § 301 (a) ab.[1728] Dieser bestimmt, dass in Fällen, in denen das streitgegenständliche Werk in den durch 17 U.S.C. §§ 102 und 103 geschützten Anwendungsbereich fällt und die Verletzung eines der in 17 U.S.C.

[1721] Scott on Multimedia Law, § 4.37 [B] [1].
[1722] Einer Klage basierend auf dem Recht eines Bundesstaates.
[1723] Deutsch: Fahrlässigkeitslehre.
[1724] Watkins, Wireless Liability, S. 16 (2013).
[1725] Watkins, Wireless Liability, S. 16 (2013).
[1726] Watkins, Wireless Liability, S. 16 (2013).
[1727] Liberty Media Holdings, LLC v. Tabora, July 9, 2012, 12 Civ. 2234 (LAK) (S.D. New York), einsehbar unter https://docs.justia.com/cases/federal/district-courts/new-york/nysdce/1:2012cv02234/393886/33/, zuletzt besucht am 24.04.2016.
[1728] Sog. „federal preemption doctrine", 17 U.S.C. § 301: *„[...] all legal or equitable rights that are equivalent to any of the exclusive rights within the general scope of copyright as specified by section 106 in works of authorship that are fixed in a tangible medium of expression and come within the subject matter of copyright as specified by section 102 and 103, [...], are governed exclusively by this title."*

§ 106 geschützten exklusiven Rechte geltend gemacht wird, ausschließlich der *Copyright Act of 1976* als Bundesgesetz Anwendung findet.

Der Kläger stützte seinen Anspruch im vorliegenden Fall auf eine *contributory copyright infringement*, welche in den Anwendungsbereich des Bundesgesetzes fällt und somit eine Klage aufgrund Fahrlässigkeit nach *state law* ausschließt.[1729] Entsprechend wurde die Klage abgewiesen.

Denkbar wären folglich eine Haftung wegen *contributory* oder *vicarious infringement* oder aufgrund von *inducement*.

Für eine *contributory liability* dürfte es regelmäßig bereits an der erforderlichen Kenntnis der Rechtsverletzung fehlen.[1730] Derjenige, der Dritten ein offenes WLAN zur Verfügung stellt, hat prinzipiell keine Kenntnis darüber, auf welche Weise diese Dritten die Internetverbindung nutzen. In Betracht käme lediglich eine Kenntnis aufgrund eines vorherigen Hinweises über eine Rechtsverletzung durch den Urheberrechtsinhaber. Auch ist fraglich, ob in der Zurverfügungstellung eines offenen WLAN eine *material contribution* gesehen werden kann. Wie bereits hinsichtlich des Access-Providers festgestellt, wäre auch bei einer weiten Auslegung der bislang aufgestellten Grundsätze einer *contributory liability* fraglich, ob ein Gericht eine *material contribution* in der Zurverfügungstellung des Anschlusses bzw. der technischen Infrastruktur sieht.

Auch eine *vicarious liability* wird aufgrund der fehlenden Kontrolle des WLAN-Anschlussinhabers sowie aufgrund des fehlenden finanziellen Interesses an einer Rechtsverletzung in der Regel zu verneinen sein.[1731] Und sofern der Anschlussinhaber sein WLAN nicht mit der Absicht bereithält, Dritten hierüber

[1729] Liberty Media Holdings, LLC v. Tabora, July 9, 2012, 12 Civ. 2234 (LAK) (S.D. New York), S. 4 f., einsehbar unter https://docs.justia.com/cases/federal/district-courts/new-york/nysdce/1:2012cv02234/393886/33/, zuletzt besucht am 24.04.2016.
[1730] So auch Watkins, Wireless Liability, S. 22 (2013).
[1731] So auch Watkins, Wireless Liability, S. 24 (2013).

Urheberrechtsverletzungen zu ermöglichen, dürfte auch kein Fall von *inducement* vorliegen.[1732]

Eine Verantwortlichkeit des WLAN-Anschlussinhabers für Urheberrechtsverletzungen durch Dritte ist demnach grundsätzlich im Rahmen der *contributory liability* möglich, nach den bisherigen durch die Rechtsprechung aufgestellten Maßstäben allerdings unwahrscheinlich.

6. Strafrechtliche Verantwortlichkeit des Access-Providers

Die strafrechtliche Verantwortlichkeit des Access-Providers setzt eine vorsätzliche Urheberrechtsverletzung, welche auf den wirtschaftlichen Vorteil bzw. der privaten finanziellen Bereicherung ausgelegt ist voraus. Strafrechtliche Verfahren gegen Access-Provider sind bislang nicht bekannt und auch hinsichtlich der üblicherweise neutralen Tätigkeit eher unwahrscheinlich. Um strafrechtlich belangt zu werden, müsste der Access-Provider vorsätzlich selbst oder mit Hilfe eines anderen, bspw. dem Nutzer des Services, mit Wissen und Wollen eine Urheberrechtsverletzung begehen.

7. Zivilrechtliche Verantwortlichkeit der Information Location Tools

Information Location Tools könnten durch die von ihnen zur Verfügung gestellten Dienste für die Verletzung des *reproduction rights* (Vervielfältigungsrecht) sowie des *rights to display the work publicly* (das Recht das Werk öffentlich anzuzeigen) verantwortlich sein.

a) Direct infringer

Eine Haftung als *direct infringer* wird im Falle des *Information Location Tools* in der Regel ausgeschlossen sein.

In *Perfect 10 v. Amazon* hat der *Ninth Circuit* zunächst eine direkte Rechtsverletzung hinsichtlich der Vorschaubilder-Anzeige von Google bejaht.[1733] Nach dem sog. *server test* wird ein

[1732] So auch Watkins, Wireless Liability, S. 24 (2013).
[1733] Perfect 10, Inc. v. Amazon.com, Inc., 508 F.3d 1146, 1160 (2007).

Urheberrechtswerk öffentlich abgebildet sofern der Inhaber eines Computers dieses als elektronische Information speichert und diese direkt dem Nutzer zur Verfügung stellt.[1734] Da Google die Vorschaubilder selbst kreiert, auf seinen Servern speichert und auf Suchanfrage des Nutzers diesem durch Anzeige des Vorschaubildes reagiert, ist ein *publicly display* der urheberrechtlich geschützten Fotos gegeben.[1735] Eine Verantwortlichkeit als *direct infringer* scheiterte aber an der Schrankenbestimmung des *fair use*.[1736]

Google's in-line linking hingegen stellt nach Ansicht des *Ninth Circuit* keine direkte Urheberrechtsverletzung dar, da Google hier keine Kopie des Fotos im Sinne des Urheberrechtsgesetzes auf seinen Servern speichert, sondern lediglich HTML Instruktionen bereithält, welche den Browser des Nutzers auf die Webseite leiten, die tatsächlich das Foto speichert.[1737] Es sei unerheblich, dass Nutzer durch den in-line Link den Eindruck gewinnen, dass der Inhalt direkt auf der Google Seite eingebunden ist, da das Urheberrechtsgesetz den Urheberrechtsinhaber nicht gegen Handlungen schützt die eine Verwechslungsgefahr beim Kunden hervorrufen.[1738]

b) Indirect infringer

Nach Auffassung des *Ninth Circuit* ist eine Haftung Googles für das in-line linking als contributory infringer möglich, sofern Google Kenntnis über die rechtsverletzenden Inhalte hat, einfache Schritte unternehmen kann, um weiteren Schaden für den Urheberrechtsinhaber zu verhindern und es unterlassen hat, solche Schritte zu unternehmen.[1739]

[1734] Perfect 10, Inc. v. Amazon.com, Inc., 508 F.3d 1146, 1159 (2007); *„[...] a computer owner that stores an image as an electronic information and serves that electronic information directly to the user (i.e., physically sending ones and zeroes over the Internet to the user's browser, Perfect 10, 416 F.Supp.2d at 839) is displaying the electronic information in violation of a copyright holder's exclusive display right."*

[1735] Perfect 10 v. Google, Inc., 416 F. Supp. 2d 828, 844 (C.D. Cal.).

[1736] Perfect 10 v. Amazon.com, Inc., 508 F. 3d 1146, 1168 (2007).

[1737] Perfect 10 v. Amazon.com, Inc., 508 F. 3d 1146, 1160 f. (2007).

[1738] Perfect 10 v. Amazon.com, Inc., 508 F. 3d 1146, 1161 (2007).

[1739] Perfect 10 v. Amazon.com, Inc., 508 F. 3d 1146, 1172 (2007).

Eine Haftung aufgrund *vicarious infringement* hat der Ninth Circuit in diesem Fall abgelehnt, da Google keine Kontrolle über den direkten Rechtsverletzer besaß und entsprechend kein Recht und keine Möglichkeit hatte, die direkte Rechtsverletzung auf der Webseite eines Dritten zu beenden.[1740]

Civilini geht daher davon aus, dass die Hürde der Beweislast letzten Endes so hoch ist, dass eine Haftung der Suchmaschine unwahrscheinlich ist.[1741]

Hinsichtlich einer auf die Auffindung von Musikdateien spezialisierten Suchmaschine führte der *S.D.N.Y.* aus, dass diese sowohl aufgrund *contributory* und *vicarious liability* haften könnte.[1742] Das Gericht begründete dies damit, dass hinsichtlich der *contributory liability* wesentliche Aspekte bestanden, welche dafür sprachen, dass die Suchmaschine sowohl Kenntnis von den Rechtsverletzungen hatte als auch wesentlich dazu beitrug.[1743] Hinweise auf ein Kennenmüssen der Rechtsverletzungen sah das Gericht unter anderem in der großen Anzahl von Links, dessen Bezeichnung auf offensichtlich rechtswidrige Inhalte hinwies sowie in dem Anerkenntnis der Manager, dass eine statistische Wahrscheinlichkeit besteht, dass einige der verlinkten Inhalte urheberrechtswidrig sind, auch eine tatsächliche Kenntnis aufgrund der durch den Rechteinhaber gesendeten *notifications* sei nicht auszuschließen.[1744] Der wesentliche Beitrag zu den Urheberrechtsverletzungen liege in der Zurverfügungstellung der Suchmaschine für Audiodateien, dem Werben damit, Links zu Seiten mit Audiodateien hochzuladen sowie die Tatsache, dass Mitarbeiter der Suchmaschine auf Anfrage von Nutzern nach MP3-Dateien suchten und diese anschließend verlinkten.[1745]

[1740] Perfect 10 v. Amazon.com, Inc., 508 F. 3d 1146, 1175 (2007).
[1741] Civilini, 19 UCLA Ent. L. Rev. 407, 434 (2012).
[1742] Arista Records, Inc. v. MP3 Board, Inc., 2002 U.S. Dist. LEXIS 16165 (S.D.N.Y. 2002), 00 Civ. 4660.
[1743] Arista Records, Inc. v. MP3 Board, Inc., 2002 U.S. Dist. LEXIS 16165 (S.D.N.Y. 2002), 00 Civ. 4660, at *15.
[1744] Arista Records, Inc. v. MP3 Board, Inc., 2002 U.S. Dist. LEXIS 16165 (S.D.N.Y. 2002), 00 Civ. 4660, at *20 ff.
[1745] Arista Records, Inc. v. MP3 Board, Inc., 2002 U.S. Dist. LEXIS 16165 (S.D.N.Y. 2002), 00 Civ. 4660, at *16 ff.

Auch eine *vicarious liability* schloss der *S.D.N.Y.* nicht aus. Das Recht und die Möglichkeit der Kontrolle bestand darin, dass die Suchmaschine den Zugang seiner Nutzer zu einer bestimmten Quelle jederzeit sperren sowie Links hierzu entfernen konnte.[1746] Ein direktes finanzielles Interesse sah das Gericht in der Tatsache, dass die Einnahmen aus der Werbung direkt mit der Anzahl der Nutzer verknüpft war, die die Seite besuchten sowie daran, dass der Dienst ausschließlich dem Auffinden von Musikdateien gewidmet sei, im Unterschied zu einer allgemeinen Suchmaschine.[1747]

Grundsätzlich ist insbesondere bei einer auf Musik- bzw. Videodateien spezialisierten Suchmaschine eine Haftung auf Grundlage der *inducement liability* möglich. Dies ist beispielsweise denkbar, sofern der Suchmaschinenanbieter absichtlich auf urheberrechtsverletzende Inhalte verlinkt mit der Absicht der Förderung von Rechtsverletzungen.

8. Strafrechtliche Verantwortlichkeit der Information Location Tools

Auch eine strafrechtliche Verantwortlichkeit des *Information Location Tools* ist denkbar.

Zwei Fälle sind bekannt, in denen gegen *Information Location Tools* vorgegangen wurde, die jeweils eine Webseite unterhielten, die auf urheberrechtswidriges Material verlinkte. Im Fall *Rojadirecta* beschlagnahmte die *Immigration and Customs Enforcement Agency* (ICE) des *U.S. Department of Homeland Security* die Domains rojadirecta.com und rojadirecta.org wegen strafbarer Verletzung von Urheberrechten.[1748] Ob tatsächlich die Tätigkeit von Project 80, nämlich das Verlinken auf urheberrechtswidrige Inhalte, als strafrechtliche Urheberrechtsverletzung angesehen werden kann, wurde nie

[1746] Arista Records, Inc. v. MP3 Board, Inc., 2002 U.S. Dist. LEXIS 16165 (S.D.N.Y. 2002), 00 Civ. 4660, at *33 ff.
[1747] Arista Records, Inc. v. MP3 Board, Inc., 2002 U.S. Dist. LEXIS 16165 (S.D.N.Y. 2002), 00 Civ. 4660, at *35 ff.
[1748] Siehe Affidavit in Support of Application for Seizure Warrant, United States v. Rojadirecta.com, 2011 WL 320195 (S.D.N.Y. Jan 31, 2011) (No. 11-MAG-262).

entschieden, da die Behörde die Domains letztendlich nach 20 Monaten wieder freigab und die Klage fallen ließ.[1749]

Auch in dem Fall *TVShack*, eine Webseite, auf der Links zu Fernsehinhalten dritter Seiten von Dritten zur Verfügung gestellt wurden, wurde die Domain tvshack.net von der ICE beschlagnahmt und der Betreiber anschließend wegen strafbarer Urheberrechtsverletzung angeklagt.[1750] Auch in diesem Fall wurde die Strafbarkeit des Verlinkens zu urheberrechtlich geschützten Werken nicht abschließend geklärt, da die Parteien ein sog. *Deferred Prosecution Agreement*[1751] schlossen.[1752] Dies ist vor dem Hintergrund bedauernswert, dass hierdurch eine eingehende gerichtliche Auseinandersetzung mit den Einzelheiten des Falls vermieden wurde und somit die Frage, ob und unter welchen Umständen *Information Location Tools* strafrechtlich verantwortlich für die Bereitstellung eines Dienstes sind.

Sofern *Information Location Tools* vorsätzlich mit den Nutzern zusammenarbeiten, die Links auf ihren Seiten zur Verfügung stellen, wäre ein *aiding and abetting* im strafrechtlichen Sinne grundsätzlich möglich, insbesondere durch *inducement*. Fraglich ist allerdings zu welcher urheberrechtlichen Verwertungshandlung der Anbieter der Linksammlungen verleitet. Denn um bei einer urheberrechtlichen Verletzungshandlung Beihilfe zu leisten, muss es zunächst einen direkten Rechtsverletzer geben, welcher das Urheberrecht durch seine Handlung verletzt. Dies ist beim Linken zu Inhalten durchaus fraglich. Der *Seventh Circuit* hat diese

---

[1749] Verfügung des U.S. District Court Southern District of New York einsehbar unter http://www.wired.com/images_blogs/threatlevel/2012/08/Endorsed-Order-Vacating-Seizure-Warrants.pdf, zuletzt besucht am 24.04.2016. Zur Möglichkeit der Beschlagnahme von Webseiten durch ICE, siehe E.IV.1.a).

[1750] United States of America v. Richard J. O'Dwyer, Klage einsehbar unter http://isites.harvard.edu/fs/docs/icb.topic1210912.files//U-S-v-O-Dwyer-SDNY-1-Sealed-Complaint.pdf, zuletzt besucht am 24.04.2016.

[1751] Ein „Deferred Prosecution Agreement" ist eine Vereinbarung zwischen dem Beklagten und der Staatsanwaltschaft, in welcher bestimmt wird, dass die Anklage gegen den Beklagten bei Erfüllung bestimmter Voraussetzungen fallen gelassen wird, siehe http://www.sao8.org/DeferredProsecution.htm, zuletzt besucht am 24.04.2016.

[1752] Siehe hierzu BBC News, Richard O'Dwyer 'happy' US copyright case is over, http://www.bbc.com/news/uk-england-20636626, zuletzt besucht am 24.04.2016.

Konstellation in dem Fall *Flava Works v. Gunter* beleuchtet und ist hier zu zwei verschiedenen Interpretationen gelangt.[1753] Es wäre zunächst denkbar, dass das Hochladen eines Videos eine öffentliche Aufführung des Werkes darstellt, welches den Nutzern ermöglicht sich das Werk nach Belieben anzuschauen.[1754] Das Gericht nennt diese Interpretation *performance by uploading*.[1755] Die alternative Interpretation geht davon aus, dass die öffentliche Aufführung lediglich eintritt, sobald das Werk auf dem Computer des Nutzers übertragen wird, sog. *performance by receiving*.[1756] In ersterem Fall spiele der Webseitenbetreiber von Linksammlungen keine Rolle im Hinblick auf das betroffene Verwertungsrecht, da es keine Beweise gebe, dass er auf die Entscheidung des Uploaders, ein bestimmtes Video im Internet hochzuladen, hinwirke während es bei zweiterem Argumente gebe, die dafür sprechen, dass der Webseitenbetreiber durch das Bereithalten des Links seine Nutzer bei der Übertragung des Werkes auf deren Computer unterstützt und damit auch die Verletzung des Rechts der öffentlichen Aufführung.[1757]

Nimmer gibt zu Bedenken, dass die Urteilsbegründung des Gerichts nicht auf die potentielle Verletzung des Vervielfältigungsrechts eingeht.[1758] So sei denkbar, dass der Nutzer der Webseite mit den Linksammlungen durch das Anklicken des Links selbst eine Vervielfältigung des Werkes auf seinem Computer vornimmt.[1759]

Zudem ist folgende Situation vorstellbar: Wird ein Video in einem gesicherten privaten Schließfach hochgeladen, welches ohne entsprechenden Link nicht von anderen Personen abrufbar ist und stellt der Schließfachinhaber daraufhin den Link hierzu auf der Webseite bereit, so ist es durchaus vertretbar, erst durch die Linksetzung auf der Webseite von einer öffentlichen Aufführung auszugehen. In diesem Fall wäre dann auch eine Beihilfe des

[1753] Flava Works, Inc., v. Gunter, 689 F.3d 754 (2012).
[1754] Flava Works, Inc., v. Gunter, 689 F.3d 754, 760 (2012).
[1755] Flava Works, Inc., v. Gunter, 689 F.3d 754, 760 (2012).
[1756] Flava Works, Inc., v. Gunter, 689 F.3d 754, 760 (2012).
[1757] Flava Works, Inc., v. Gunter, 689 F.3d 754, 761 (2012).
[1758] Nimmer on Copyright, § 12B.05 [A] [1].
[1759] Nimmer on Copyright, § 12B.05 [A] [1].

Webseitenbetreibers hinsichtlich der Verletzung des Rechts der öffentlichen Aufführung nicht ausgeschlossen.

V. Selbstregulatorische Maßnahmen der ISP

1. User Generated Content Principles

Im Jahr 2007 haben sich verschiedene Urheberrechtsinhaber sowie ISP, die nutzergenerierte Inhalte (*user generated content*) auf ihren Plattformen zur Verfügung stellen, die sog. *User Generated Content Principles* (*UGC Principles*) veröffentlicht.[1760] Diese legen als sog. *best practices* verschiedene Prinzipien zur Erreichung der folgenden Ziele fest:

(1) die Beseitigung von rechtsverletzenden Inhalten auf UGC-Plattformen;

(2) die Förderung von originellen und zulässigen nutzergenerierten Audio- und Videoinhalten;

(3) die Berücksichtigung von *fair use*-Inhalten auf UGC-Plattformen;

(4) den Schutz berechtigter Datenschutzinteressen der Nutzer.

Die UGC Principles bestehen aus insgesamt 15 Grundsätzen, welche die Regelungen des DMCA *safe harbor* ergänzen sollen.[1761] So sollen die UGC-Plattformen beispielsweise Informationen zur Förderung der Achtung von geistigen Eigentumsrechten auf ihrer Seite posten, Nutzer während des Upload-Prozessen über das Verbot des Hochladens rechtsverletzender Inhalte informieren und von diesen eine entsprechende Zustimmung hinsichtlich der Achtung von geistigen Eigentumsrechten einholen sowie Technologie zur Identifizierung von Inhalten einsetzen.

Im Gegenzug verpflichten sich die Urheberrechtsinhaber dazu, nicht gegen diejenigen UGC-Plattformen wegen Verletzung von Urheberrechten vorzugehen, welche die Prinzipien einhalten.

[1760] Einsehbar unter http://www.ugcprinciples.com, zuletzt besucht am 24.04.2016, zu den Initiatoren zählten u.a. UGC Services wie MySpace, Dailymotion und Veoh.com.

[1761] Ballon, 4.12[17][A].

2. Copyright Alert System

Individuelle Internetnutzer und deren Aktivitäten in Peer-to-Peer Filesharing Netzwerken standen seit 2003 im Fokus der Content-Industrie.[1762] Während sie sich anfangs noch der *subpoena*-Bestimmung des DMCA zur Identifizierung potentieller Rechtsverletzer bediente, ging sie nach einem Urteil des *D.C. Circuit*[1763] einen anderen Weg und reichte John Doe-Klagen gegen die vermeintlichen Rechtsverletzer ein. Oftmals mit der Forderung nach dem maximal möglichen Schadensersatz gem. 17 U.S.C. § 504 (c) (2) von $ 150.000 pro vorsätzlicher Verletzung von Urheberrechten.[1764] Auch wenn der geforderte Schadensersatz von $ 150.000 pro Werk von den Gerichten nicht zugesprochen wurde, sprachen die Gerichte der Content-Industrie Ansprüche im Bereich von $ 750 bis $ 9.250 pro Werk zu, was teilweise zu Gesamtschadensersatzansprüchen von $ 220.000 führte.[1765] Da die Content-Industrie bei ihrem Feldzug gegen individuelle Peer-to-Peer Nutzer jedoch unterschiedslos sowohl gegen notorische Rechtsverletzer als auch gegen sog. *sympathetic groups* wie ältere Personen, Arme und Minderjährige vorging, geriet die Vorgehensweise in der Öffentlichkeit zunehmend unter Kritik.[1766]

Im Jahr 2008 erklärte die Musikindustrie schließlich einen Richtungswechsel und fokussierte sich fortan auf mögliche Kooperationsmaßnahmen mit den ISP.[1767]

Nachdem bereits 2011 der Grundstein für eine Kooperation zwischen Rechteinhabern und ausgewählten Access-Providern in Form eines *Memorandum of Understanding*[1768] gelegt wurde, begann Anfang des Jahres 2013 die Implementierungsphase des

---

[1762] Schneidman, 23 J.L. & Pol'y 397, 405 (2014).

[1763] Recording Industry Association of America, Inc., v. Verizon Internet Services, Inc., 351 F.3d 1229, 1238 (D.C. Cir. 2003), der *D.C. Circuit* erklärte hier § 512 (h) DMCA unanwendbar auf Access-Provider, siehe hierzu D.III.5.j).

[1764] Schneidman, 23 J.L. & Pol'y 397, 406 (2014).

[1765] Schneidman, 23 J.L. & Pol'y 397, 407 ff. (2014).

[1766] Schneidman, 23 J.L. & Pol'y 397, 408 (2014).

[1767] Schneidman, 23 J.L. & Pol'y 397, 410 (2014).

[1768] Einsehbar unter http://www.copyrightinformation.org/wp-content/uploads/2013/02/Memorandum-of-Understanding.pdf, zuletzt besucht am 24.04.3016.

sog. *Copyright Alert Systems* in den USA.[1769] Selbsterklärtes Ziel ist die Bekämpfung von Online-Piraterie unter Berücksichtigung der legitimen Interessen der Internetnutzer, dem Schutz ihrer Privatsphäre und Meinungsfreiheit, der Beachtung des Zugangs zu rechtmäßigen Inhalten und der Möglichkeit des Nutzers gegen falsche Behauptungen vorzugehen.[1770]

a) Funktionsweise des Copyright Alert System

Das *Copyright Alert System* beruht auf einer privatrechtlichen Vereinbarung zwischen fünf großen US-amerikanischen Access-Providern und Rechteinhabern, wie bspw. der *Recording Industry Association of America* (RIAA) und der *Motion Picture Association of America* (MPAA).[1771] Zur Umsetzung wurde das *Center for Copyright Information* (CCI) gegründet.[1772] Nach dem „*Six-Strikes*"-Warnsystem erhalten Nutzer bei einer Urheberrechtsverletzung bis zu 6 Warnmeldungen. Der Access-Provider hat nach mehrmaliger Verwarnung die Möglichkeit, Sanktionen gegen den Nutzer durchzusetzen (*mitigation measures*), wie bspw. eine vorübergehende Drosselung der Internetgeschwindigkeit oder die Weiterleitung auf eine Vorschalteseite, auf welcher der Nutzer dazu aufgefordert wird, ein Online-Urheberrechtsschulungsseminar zu absolvieren (sog. *mitigation stage*).[1773] Es ist umstritten, ob im Rahmen der *mitigation stage* auch eine vorübergehende Unterbrechung des Internetzugangs möglich ist.[1774] Gemäß den Bestimmungen des *Memorandum of Understanding* ist jedoch davon auszugehen, dass es den Access-Providern offen steht, auch eine zeitweise

[1769] Lesser, Copyright Alert System Set to Begin.
[1770] Memorandum of Understanding, Preamble.
[1771] Details über das Copyright Alert System sind unter http://www.copyrightinformation.org/about-cci/ einsehbar, zuletzt besucht am 24.04.2016.
[1772] Siehe hierzu http://www.copyrightinformation.org, zuletzt besucht am 24.04.2016.
[1773] Siehe http://www.copyrightinformation.org/the-copyright-alert-system/what-is-a-copyright-alert/, zuletzt besucht am 24.04.2016.
[1774] Bejahend: Bridy, 23 Fordham Intell. Prop. Media & Ent. L.J. 1, 32 (2012); Verneinend: Schneidman, 23 J.L. & Pol'y 397, 431 (2014).

Unterbrechung des Internetzugangs als *mitigation measure* einzuführen.[1775]

Im Rahmen der *mitigation stage* steht es dem Internetnutzer offen, Einspruch einzulegen. Die jeweilige im Rahmen der Warnmeldung erwähnte Sanktion wird entsprechend erst nach dem Ablauf von 14 Kalendertagen umgesetzt.[1776] Entscheidet sich der Internetnutzer zum Einspruch, richtet sich das weitere Vorgehen nach den Regeln des *Independent Review Program*.[1777] Der Internetnutzer kann seinen Einspruch demnach auf folgende sechs Verteidigungen stützen: (1) *Misidentification of Account*, (2) *Unauthorized Use of Account*, (3) *Authorization*, (4) *Fair Use*, (5) *Misidentification of File* oder (6) *Work Published Before 1923*.

Die *Independent Review* erfolgt durch einen einzelnen unabhängigen Gutachter, welcher von der *American Arbitration Association* gestellt wird.[1778]

Die administrativen Kosten des *Independent Review Program* tragen zu 50% die am *Copyright Alert System* beteiligten Rechteinhaber sowie zu 50% die hieran beteiligten Access-Provider.[1779] Der Internetnutzer hat zudem eine administrative *Filing Fee* in Höhe von $ 35 zu tragen.[1780]

b) Kritik

In der Kritik steht vornehmlich der privatrechtliche Charakter des *Copyright Alert Systems* und die damit einhergehende

---

[1775] Memorandum of Understanding, 4.G.(iii), *„[...] such other temporary Mitigation Measure as may be applied b the Participating ISP in its discretion that is designed to be comparable to those Mitigation Measures discribed above.“; so auch beispielsweise bei dem Access-Provider Optimum: „CAS Alerts may result in a temporary suspension of Optimum Online service.“*, siehe http://optimum.custhelp.com/app/answers/detail/a_id/3592/kw/copyright, zuletzt besucht am 24.04.2016.

[1776] Siehe Memorandum of Understanding, 4.G.(iii).

[1777] Siehe Memorandum of Understanding, Attachment C.

[1778] Siehe Memorandum of Understanding, Attachment C, 4.2.1. sowie Pressemitteilung der CCI vom 02. April 2012, einsehbar unter http://www.copyrightinformation.org/press-release/center-for-copyright-information-announces-three-major-steps-towards-implementation/, zuletzt besucht am 24.04.2016.

[1779] Siehe Memorandum of Understanding, 4.H.(ii).

[1780] Siehe Memorandum of Understanding, Attachment C, 4.1.6, diese kann in Ausnahmefällen reduziert oder ganz erlassen werden.

Privatisierung der Rechtsdurchsetzung.[1781] So hat der Internetnutzer erst ab der *mitigation stage* die Möglichkeit, gegen eine unberechtigte Meldung des Rechteinhabers vorzugehen. Bei den vorherigen Warnmeldungen besteht keine Möglichkeit des Einspruchs.

Zudem kommt es im Rahmen des *Independent Review Program* zu einer Beweislastumkehr zu Lasten des Internetnutzers.[1782] Während es im Rahmen eines gerichtlichen Urheberrechtsverletzungsverfahrens dem Urheberrechtsinhaber obliegt, eine behauptete Rechtsverletzung nachzuweisen, wird im Rahmen des *Copyright Alert Systems*, eine Urheberrechtsverletzung durch den Internetnutzer vermutet, so dass es diesem nun obliegt, nachzuweisen, dass er nicht das Urheberrecht verletzt hat.

Zudem kann der Internetnutzer im Rahmen des *Independent Review Program* lediglich die sechs festgelegten Einwendungen vorbringen. Das Urheberrechtsgesetz sieht aber grundsätzlich mehr potentielle Einwendungen vor.[1783]

Schneidman macht überdies geltend, dass das *Copyright Alert System* zu einer unangemessenen Benachteiligung von Kleinunternehmern (*small business owners*) führen kann.[1784] Nach dem Wortlaut des *Memorandum of Understanding*[1785] sowie nach eigener Aussage des CCI[1786] wird das *Copyright Alert System* gegenüber *residential Internet accounts*, also private Haushalte, angewandt und nicht gegenüber *business accounts,* also gegenüber Unternehmern. Gerade kleine Unternehmen, wie bspw. Coffee

---

[1781] Bridy, 23 Fordham Intell. Prop. Media & Ent. L.J. 1, 37f. (2012); Storch, 16 Stan. Tech. L. Rev. 453, 469 (2013); Flaim, 2 N.Y.U. J. of Intell. Prop. & Ent. Law 142, 164 (2012).

[1782] Bridy, 23 Fordham Intell. Prop. Media & Ent. L.J. 1, 34 (2012).

[1783] Bridy, 23 Fordham Intell. Prop. Media & Ent. L.J. 1, 57 f. (2012), beispielsweise können Urheberrechtswerke bereits in der public domain sein auch wenn sie nach 1923 veröffentlicht wurden.

[1784] Schneidman, 23 J.L. & Pol'y 397, 445 (2014).

[1785] Memorandum of Understanding, Preamble *„[...] consumer-focused process for identifying and notifying residential wired Internet access service customers [...]"*.

[1786] Blog Post vom Jill Lesser, einsehbar unter http://www.copyrightinformation.org/uncategorized/cas-will-not-harm-public-wi-fi/, zuletzt besucht am 24.04.2016.

Shops, Restaurants, Bars, Friseur Salons oder Buchhandlungen verfügen aber oftmals über keinen *business account*, sondern lediglich über einen *residential Internet account*.[1787] Daher besteht grundsätzlich auch für diese die Gefahr, Empfänger einer Warnmeldung zu werden und den damit verbundenen Maßnahmen ausgesetzt zu sein. Zwar haben auch Kleinunternehmen grundsätzlich die Möglichkeit, Einspruch gegenüber des CCI einzulegen und eine unautorisierte Nutzung ihres Kontos geltend zu machen, allerdings kann diese Verteidigung nur ein einziges Mal vorgebracht werden, um dem Internetnutzer die Möglichkeit zu geben, in Zukunft seinen Anschluss entsprechend gegen unautorisierte Nutzung abzusichern.[1788]

Schneidman macht geltend, dass freies WLAN insbesondere für Kleinunternehmen von großer Bedeutung sei und maßgeblich zu deren Erfolg beitrage.[1789] Zudem diene freies WLAN der Gesellschaft als Ganzes und sei ein bedeutsamer wirtschaftlicher Faktor, da es Innovationen begünstige, den Tourismus befördere und Städte attraktiver mache.[1790]

c) Fazit

Auch wenn die Abkehr von der massenhaften Klageerhebung gegen individuelle Internetnutzer zu begrüßen ist, begegnet das *Copyright Alert System* nicht unerheblichen Bedenken, insbesondere im Hinblick auf die Berücksichtigung von Nutzerinteressen.

Zudem ist das System wenig transparent, so dass eine Evaluierung dahingehend, ob es die erklärten Ziele erreicht, nicht möglich ist.[1791] 2014 veröffentliche das CCI einen eigens erstellten Report mit Zahlen hinsichtlich der ersten 10 Monate des *Copyright Alert Systems*.[1792] Der Report enthält zum größten Teil Statistiken hinsichtlich der Anzahl versendeter Warnmeldungen auf den

[1787] Schneidman, 23 J.L. & Pol'y 397, 436 (2014).
[1788] Siehe Memorandum of Understanding, Attachment C, 2.2.
[1789] Schneidman, 23 J.L. & Pol'y 397, 437 (2014).
[1790] Schneidman, 23 J.L. & Pol'y 397, 438 (2014).
[1791] So auch Bridy, 23 Fordham Intell. Prop. Media & Ent. L.J. 1, 67 (2012).
[1792] CCI, The Copyright Alert System – Phase One and Beyond.

einzelnen Stufen sowie der *Independent Review Decisions*. Aus dem Bericht geht hervor, dass in den ersten 10 Monaten nach Einführung des *Copyright Alert Systems* über 2 Millionen Mitteilungen hinsichtlich behaupteter Urheberrechtsverletzungen an die Access-Provider gesendet wurden und ca. 1,3 Millionen Warnmeldungen aufgrund dieser Mitteilungen an die Anschlussinhaber versendet wurden.[1793] Die Zahl derjenigen Nutzer, die lediglich eine Warnmeldung erhielten, liegt bei 722.820 Nutzern, während 37.456 Nutzer eine sechste Warnmeldung erhielten.[1794] Ob dies darauf zurückzuführen ist, dass die im ersten und zweiten Schritt vorgesehenen *educational alerts* Wirkung gezeigt haben, kann lediglich vermutet werden. Im Hinblick auf das *Independent Review Program* wurden 83% der Warnmeldungen bestätigt, wohingegen 18% zurückgezogen wurden.[1795] Diesbezügliche inhaltliche Details lässt der Report vermissen.

VI. Zusammenfassung

Trotz vereinzelt bestehender Unklarheiten und Unzulänglichkeiten des § 512 DMCA wurde das Ziel einer engeren Zusammenarbeit zwischen ISP und Rechteinhabern zur Aufdeckung und dem Umgang mit Online-Urheberrechtsverletzungen unter Schaffung von mehr Rechtssicherheit für ISP im Großen und Ganzen erreicht. So geht auch die wohl h.M. im Schrifttum davon aus, dass die *safe harbor*-Regelungen insgesamt als Erfolg zu werten sind[1796].

Es gibt es jedoch auch Stimmen in der Literatur, die davon ausgehen, dass insbesondere hinsichtlich des Host-Providers das erklärte Ziel des DMCA, mehr Rechtssicherheit zu schaffen, nicht erreicht wurde.[1797] Dies ist größtenteils zurückzuführen auf die

[1793] CCI, The Copyright Alert System – Phase One and Beyond, S. 4.
[1794] CCI, The Copyright Alert System – Phase One and Beyond, S. 9.
[1795] CCI, The Copyright Alert System – Phase One and Beyond, S. 11.
[1796] So z.B. Carroll, U. Miami L. Rev. 421, 443 (2014); Mlynar, 19 Intell. Prop. L. Bull. 1, 1 (2014); Notice and Takedown in Everyday Practice, S. 115; Wiseman, 14 Nev. L.J. 210, 215 (2013).
[1797] Helman/Parchomovsky, 111 Colum. L. Rev. 1194, 1205 (2011); Reese, 34 Sw. U. L. Rev. 287, 323 (2004).

Verwendung unbestimmter Rechtsbegriffe im DMCA.[1798] Rechteinhaber nutzen dies aus, um eine Entscheidung im Rahmen des *summary judgements* zu verhindern und damit ein ordentliches Gerichtsverfahren einzuleiten und die Prozesskosten in die Höhe zu treiben.[1799] Dies ist insbesondere für Start-up Unternehmen oder Unternehmen mit geringerer Finanzkraft problematisch, die den oftmals sehr liquiden Vertretern der Musik- oder Filmindustrie gegenüberstehen. Für die ISP läuft dies trotz etwaigen Obliegens auf die potentielle Gefahr eines Bankrotts hinaus.[1800] Zudem haben sie das Damoklesschwert exorbitanter Schadensersatzforderungen über sich schweben. Diese können sich auf bis zu $ 150.000 pro Werk belaufen.[1801] Beide Aspekte sind letzten Endes auch dazu geeignet, zu einer unkritischen und vorschnellen Löschung von Inhalten durch den ISP beizutragen.[1802]

Die Gefährdung der Informations- und Meinungsfreiheit ist auch immer wieder Anlass für Kritik an dem *Notice and Takedown*-Systems. Der ISP hat das Material nach Erhalt einer formal den Anforderungen des § 512 (c) (3) (A) DMCA entsprechenden *notification* zu entfernen bzw. zu sperren, ohne dass es darauf ankommt, ob das Material tatsächlich Urheberrechte verletzt oder nicht. Dies wird teilweise ausgenutzt, um unliebsames Material zu entfernen.

Aus diesem Grund wurde im Jahr 2001 das Projekt *Lumen*[1803] gestartet, welches mittlerweile durch Kollaboration verschiedener U.S. amerikanischer *law school clinics*[1804] und der *Electronic Frontier Foundation*[1805] betrieben wird.[1806] *Lumen* sammelt und analysiert u.a. unter dem DMCA versendete *notifications.* ISP die

[1798] Blevins, 34 Cardozo L. Rev. 1821, 1878 (2013).
[1799] Blevins, 34 Cardozo L. Rev. 1821, 1829 (2013).
[1800] So bspw. geschehen bei der Videoplattform Veoh, siehe hierzu Blevins, 34 Cardozo L. Rev. 1821, 1830 f. (2013).
[1801] 17 U.S.C. § 504 (c) (2).
[1802] So auch Blevins, 34 Cardozo L. Rev. 1821, 1874 f. (2013).
[1803] Bis Ende 2015 noch unter dem Namen *Chilling Effects*.
[1804] Bspw. der Harvard University, der University of California, Berkeley, der Stanford University und der University of San Francisco.
[1805] Ein Non-Profit-Unternehmen, das sich für die Grundrechte in der digitalen Welt einsetzt, siehe https://www.eff.org, zuletzt besucht am 24.04.2016.
[1806] Siehe https://lumendatabase.org, zuletzt besucht am 24.04.2016.

eine *notification* erhalten haben, können diese unter Angabe der Details über die Webseite von *Lumen* einreichen.[1807] Ziel ist es, durch die Zurverfügungstellung einer Datenbank über sämtliche gemeldeten *notifications*, das *Notice and Takedown*-System transparenter für die allgemeine Öffentlichkeit zu gestalten und das Missbrauchspotential des Systems aufzuzeigen.[1808]

„Glänzende" Beispiele dieses Missbrauchspotentials honoriert die *Electronic Frontier Foundation* auf einer eigens eingerichteten URL, der *Takedown Hall of Shame*.[1809] Hierunter ist ein großes Musiklabel, das die *notification* dazu nutzte die kritische Auseinandersetzung einer Bloggerin mit den Songtexten eines bekannten Rappers zu unterbinden[1810], das Tourismusbüro einer kanadischen Provinz, das den Trailer eines kritisch-satirischen Films über das Ölsandprojekt dieser Provinz zu verhindern versuchte[1811] sowie der Schlagzeilen generierende Fall des *Dancing Baby,* welcher bis zum Berufungsgericht des *Ninth Circuit* ausgefochten wurde.[1812]

Neben vorsätzlich fehlerhaft versendeten *notifications*, ist ein weiterer Teil unberechtigter *notifications* dem Umstand geschuldet, dass Rechteinhaber dazu übergegangen sind, durch automatisierte Verfahren Urheberrechtsverletzungen aufzudecken und anschließend ohne menschliche Überprüfung *notifications* zu versenden.[1813]

Bedenklich sind auch die Folgen der Nichtanwendbarkeit der *counter notification* sowie des *put back procedures* auf *Information Location Tools*. Derjenige, der einer Urheberrechtsverletzung bezichtigt wird und dessen Material auf Grundlage einer formal korrekten *notification* entfernt bzw. gesperrt wird, hat keine gesetzlich festgeschriebene Möglichkeit dieser Entfernung bzw.

[1807] Siehe https://lumendatabase.org/notices/new, zuletzt besucht am 24.04.2016.
[1808] Siehe https://lumendatabase.org/pages/about, zuletzt besucht am 24.04.2016.
[1809] Siehe https://www.eff.org/de/takedowns, zuletzt besucht am 24.04.2016.
[1810] Siehe https://www.eff.org/de/takedowns/music-publisher-tries-muzzle-podcast-criticizing-akon, zuletzt besucht am 24.04.2016.
[1811] https://www.eff.org/de/takedowns/crude-copyright-complaints-silence-oil-company-satire, zuletzt besucht am 24.04.2016.
[1812] Lenz v. Universal Music Corp., 801 F.3d 1126 (9th Cir. 2015).
[1813] Notice and Takedown in Everyday Practice, S. 116.

Sperrung außergerichtlich entgegenzutreten. Hierdurch könnte das ansonsten sorgfältig austarierte Interessengeflecht des DMCA gestört sein. Durch das Fehlen eines direkten Vertragsverhältnisses mit dem Nutzer der *Information Location Tools* könnten diese eher geneigt sein, übereifrig Inhalte aus ihren Ergebnislisten zu entfernen, um einer Verantwortlichkeit nach den allgemeinen Gesetzen zu entkommen.[1814] Hierdurch besteht die Gefahr, dass auch rechtlich unbedenkliche Inhalte vorschnell gelöscht werden.[1815] *Walker* sieht daher auch verfassungsrechtliche Bedenken, insbesondere im Hinblick auf das *First Amendment*.[1816] Eine 2016 herausgebrachte Studie zum *Notice and Takedown*-Verfahren bestätigt im großen und ganzen diese Bedenken, hebt aber zugleich die Bedeutung dieses Verfahrens für das Ziel der Erreichung von Rechtssicherheit und damit dem Abbau von Markteintrittsbarrieren für diese Online Services hervor.[1817] Daher sei das System, trotz seiner Unzulänglichkeiten in diesem Sinne als Erfolg anzusehen.[1818]

E. Rechtsvergleich und Analyse

Die gesetzlichen Regelungen des TMG und DMCA sind insbesondere hinsichtlich des Access- und Cache-Providers größtenteils identisch. Auch die Haftungsprivilegierung des DMCA hinsichtlich des Host-Providers weist viele Gemeinsamkeiten mit dem des TMG auf. Eine Besonderheit des US-amerikanischen Rechts ist allerdings die detaillierte Festlegung eines *Notice and Takedown*-Verfahrens mit zusätzlicher Regelung der

[1814] Walker, Virginia Journal of Law & Technology, Vol. 9, No. 2, para. 46.
[1815] Walker, Virginia Journal of Law & Technology, Vol. 9, No. 2, para. 46.
[1816] Walker, Virginia Journal of Law & Technology, Vol. 9, No. 2, para. 48 ff. Der erste Zusatzartikel zur Verfassung besagt, dass der Kongress kein Gesetz verabschieden darf, welches die Religionsfreiheit, die Meinungsfreiheit, die Pressefreiheit, die Versammlungsfreiheit oder das Petitionsrecht einschränkt (*„Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances.“*).
[1817] Notice and Takedown in Everyday Practice, S. 125.
[1818] Notice and Takedown in Everyday Practice, S. 125.

Verteidigungsmöglichkeit des betroffenen Nutzers und eines entsprechenden *put back*-Verfahrens. Ein Pendant existiert im deutschen Recht nicht. Auch enthält das TMG im Gegensatz zum DMCA keine spezifische Regelungen hinsichtlich einer Haftungsprivilegierung des lediglich Verlinkenden.

Neben den materiell-rechtlichen Unterschieden, haben sich insbesondere Differenzen bei der Rechtsauslegung durch die Gerichte gezeigt. Während das vom BGH schon frühzeitig gefällte Grundsatzurteil hinsichtlich einer grundsätzlichen Unanwendbarkeit auf negatorische Ansprüche gegen den Host-Provider, die weitere Entwicklung der Rechtsprechung maßgeblich beeinflusst hat, hat sich in den USA eine ISP-freundlichere Rechtsprechung herausgebildet.

Access-Provider werden hingegen in den USA durch private Vereinbarungen stärker in die Pflicht genommen, dies allerdings auf rein freiwilliger Basis.

Der nachfolgende Rechtsvergleich behandelt zunächst die bedeutenden Einzelaspekte der allgemeinen Grundsätze beider Rechtsordnungen und geht sodann auf die einzelnen Adressaten der Haftungsprivilegien ein.

I. Allgemein

1. Umfang der Haftungsprivilegien

Entscheidender Unterschied zwischen dem deutschen und US-amerikanischen Recht ist der Umfang der Privilegierung der ISP. Während in den USA nur äußerst eingeschränkt dem ISP gerichtliche Anordnungen auferlegt werden können, sieht sich der ISP in Deutschland mit der Störerhaftung konfrontiert, welche ihm zum Teil umfangreiche Prüfpflichten abverlangt.[1819] Hierdurch wird das gesetzliche System der Haftungsprivilegierung der ISP konterkariert. Die von der Rechtsprechung entwickelten Grundsätze verdeutlichen, dass diese gänzlich unabhängig von den Privilegien der §§ 8-10 TMG entwickelt wurden und lassen diese

[1819] Siehe hierzu S. 231.

größtenteils unbeachtet. Es kann bezweifelt werden, dass dies im Sinne des europäischen Richtliniengebers ist. Denn da die für die ISP in der Praxis relevante „verschuldensunabhängige" Störerhaftung, anders als die *secondary liability* in den USA, ohnehin in der Regel keine Schadensersatzansprüche mit sich bringt, wurde den Privilegien durch die Rechtsprechung größtenteils ihre Bedeutung genommen. Lediglich das Verbot einer allgemeinen Überwachungspflicht des § 7 Abs. 2 S. 1 TMG wird regelmäßig von den Gerichten im Rahmen ihrer Beurteilung der spezifischen dem ISP aufzuerlegenden Prüfpflichten heranzogen, im Ergebnis wird eine Überwachung jedoch durch Bezugnahme auf eine vorherige spezifische Rechtsverletzung legitimiert.

Somit hat die ursprünglich zur Begrenzung der Störerhaftung begründete erforderliche Verletzung von Prüfpflichten dazu geführt, dass hierdurch dem ISP eine Art Verkehrspflichten auferlegt werden.[1820] Anders als die Verletzung von Verkehrspflichten kann die Verletzung von Prüfpflichten aber gerade keinen Schadensersatzanspruch begründen.

Die US-amerikanische Regelung hinsichtlich potentieller Anordnungen gegen den ISP berücksichtigt hingegen die Besonderheiten der digitalen Umwelt und lässt entsprechend keine Anordnungen zu, die das System des ISP beeinträchtigen, die nicht effektiv sind oder die den Zugang zu rechtmäßigem Material beeinträchtigen.[1821] Eine zukunftsgerichtete Verpflichtung zur Entfernung eines bestimmten Materials wurde abgelehnt, da dies eine Monitoring-Maßnahme darstellen würde, welche das durch den DMCA hergestellte Gleichgewicht beinträchtigen würde.[1822]

[1820] Früh schon in diese Richtung gehend: Schulze, ZUM 2000, 432, 452, welcher ausführt, dass die Entscheidung „Möbelklassiker" des BGH den Unterlassungsanspruch verschuldensabhängig machen wolle. So gibt auch *Peifer* zu bedenken, dass sich die Prüfpflicht systemwidrig als Verkehrspflicht in das Konzept der Unterlassungspflicht geschlichen habe, siehe Peifer, AfP 1/2014, 18, 23. Irrigerweise insoweit die Auffassung von *Holznagel*, dass die Prüfpflichten im Rahmen der Störerhaftung als Verkehrspflichten zu verstehen seien, siehe Holznagel, S. 102.

[1821] Siehe hierzu S. 348.

[1822] Siehe hierzu S. 299.

2. Ausschluss Rechtsverletzer

Zu den allgemeinen Qualifikationsvoraussetzungen des DMCA zählt die Implementierung und Umsetzung einer *policy* zum Ausschluss von Wiederholungstätern.[1823] Auch wenn das Gesetz dem ISP hinsichtlich des genauen Inhalts und der Umsetzung einen gewissen Spielraum lässt, bedarf es jedenfalls einer spezifischen diesbezüglichen *policy* sowie einer entsprechenden Umsetzung des Ausschlusses von Nutzern in angemessenen Fällen. Dieser Spielraum ist allerdings auch geeignet, Rechtsunsicherheiten des ISP zu schüren. Die Verwendung von unbestimmten Rechtsbegriffen ist hier insbesondere dafür geeignet, teure und langwierige gerichtliche Verfahren gegen den ISP einzuleiten, welche ihn in der Konsequenz dazu verleiten können, vermeintliche Rechtsverletzer vorschnell von der Nutzung seines Dienstes auszuschließen.

Das deutsche Recht sieht keine entsprechende Möglichkeit zum Ausschluss von Rechtsverletzern vor. Allerdings hat der EuGH die Möglichkeit des Ausschlusses eines Rechtsverletzers durch den Host-Provider ausdrücklich im Rahmen einer gerichtlichen Anordnung als wirksames und verhältnismäßiges Mittel angesehen, um zu verhindern, dass erneute derartige Rechtsverletzungen durch denselben Rechtsverletzer auftreten.[1824]

So hat auch das OLG Brandenburg hinsichtlich der Verkaufsplattform eBay eine grundsätzliche Zulässigkeit von Sperrklauseln in AGB als zulässig erachtet.[1825] Die Sperrung des Nutzers bezog sich allerdings nicht auf etwaig durch den Nutzer auf der Plattform vorgenommene Rechtsverletzungen, sondern auf den wiederholten Erhalt negativer Bewertungen anderer Nutzer.

Hinsichtlich eines Ausschlusses des Rechtsverletzers durch den Access-Provider gibt *Hoeren* zu bedenken, dass das Internet heutzutage zur Daseinsvorsorge gehöre und daher jedermann

[1823] Siehe hierzu S. 253.
[1824] Siehe hierzu S. 73.
[1825] OLG Brandenburg, MMR 2009, 262, 262; so auch KG MMR 2005, 764, allerdings zweifelnd dahingehend, ob ein solcher Ausschluss eines Nutzers ohne vorhergehende Abmahnung gerechtfertigt ist.

Zugang zu einem Grundangebot an Telekommunikationsdienstleistungen zu verschaffen sei.[1826] Der Access-Provider unterliege insoweit als Erbringer einer Universaldienstleistung i.S.d. § 84 Abs. 1 TKG einem Kontrahierungszwang, weshalb eine Kündigung aufgrund von Verstößen gegen die außerhalb des Vertrages liegenden Interessen Dritter äußerst bedenklich sei.[1827]

3. Auskunftsverpflichtung

§ 512 (h) DMCA enthält die Möglichkeit zum Erhalt einer Anordnung zur Identifizierung des vermeintlichen Rechtsverletzers gegenüber dem ISP. Dieser Auskunftsanspruch findet jedoch keine Anwendung auf Access-Provider.[1828] Bedenklich ist insofern, dass der Antrag einer solchen Anordnung keine Ausführungen hinsichtlich des materiell-rechtlichen Anspruchs erfordert. Es ist lediglich eine Kopie der *notification* beizulegen sowie eine eidesstattliche Erklärung darüber, dass der Urheberrechtsinhaber die Informationen lediglich zum Schutz seiner Urheberrechte nutzen wird. Eine inhaltliche Prüfung etwaiger urheberrechtlicher Ansprüche findet somit nicht statt.

Nach deutschem Recht hat der Urheberrechtsinhaber einen Auskunftsanspruch gegenüber dem ISP, vorausgesetzt es liegt eine offensichtliche Rechtsverletzung vor.[1829] Für den Fall, dass der Auskunftsanspruch allerdings nur unter Bezugnahme auf die Verkehrsdaten erfüllt werden kann, sieht das Gesetz eine richterliche Anordnung vor, d.h. das Gericht prüft das Vorliegen der Voraussetzungen für den Auskunftsanspruch.[1830] Diese Vorschrift ist insbesondere für den Access-Provider von Bedeutung, da dieser Informationen zur Identifizierung eines vermeintlichen Rechtsverletzers nur unter Hinzuziehung der IP-Adresse ermitteln kann. Hierdurch wird eine vorschnelle Preisgabe

[1826] Hoeren, Kurzgutachten zur BMWi-Studie, S. 14.
[1827] Hoeren, Kurzgutachten zur BMWi-Studie, S. 14f.
[1828] Siehe hierzu S. 344.
[1829] Siehe hierzu S. 205.
[1830] Siehe hierzu S. 210.

persönlicher Daten der Internetnutzer verhindert und die Nutzerinteressen werden verstärkt berücksichtigt.

Aber auch ohne Richtervorbehalt soll durch die Klarstellung, dass der ISP nur zur Auskunft verpflichtet ist, wenn eine offensichtliche Rechtsverletzung vorliegt, einem Missbrauch des Auskunftsanspruch vorgebeugt werden. Der ISP wird jedoch auch für den Fall geschützt, dass er eine Auskunft erteilt ohne dazu verpflichtet zu sein. Gem. § 101 Abs. 6 UrhG haftet der ISP in diesem Fall nur, wenn er wusste, dass er zur Auskunftserteilung nicht verpflichtet war. Die Gesetzesbegründung macht deutlich, dass diese Haftungserleichterung die Tatsache bereits berücksichtigt, dass es für den unbeteiligten Dritten oftmals schwierig sein kann, zu beurteilen, ob tatsächlich ein Auskunftsanspruch besteht. Denn auch wenn dieser lediglich bei offensichtlichen Rechtsverletzungen besteht, kann es dennoch für den ISP in bestimmten Fällen schwierig sein, eine offensichtliche Rechtsverletzung von einer nicht offensichtlichen zu unterscheiden. Die Gesetzesbegründung führt insofern hierzu aus, dass diese Haftungsprivilegierung dem Umstand Rechnung trägt, dass der Verpflichtete kaum beurteilen kann, ob überhaupt eine Rechtsverletzung vorliegt.[1831] Dies zeigt bereits, dass auch wenn grundsätzlich ein Auskunftsanspruch lediglich bei offensichtlichen Rechtsverletzungen gegeben ist, dem ISP diesbezügliche Unklarheiten nicht zu Lasten gelegt werden sollen. Er soll sich hier keinen diesbezüglich Regressforderungen Dritter ausgesetzt sehen.[1832]

Insofern scheint jedenfalls für Ansprüche auf Herausgabe von Bestandsdaten des Host-Providers erstmal die Schwelle, die derjenige, der einen Auskunftsanspruch geltend machen will, überwinden muss, nach deutschem Recht höher zu sein. Hier wird gesetzlich das Vorliegen einer offensichtlichen Rechtsverletzung gefordert, während hingegen im US-amerikanischen Recht lediglich eine eidesstattliche Erklärung dahingehend, dass die

[1831] BT-Drucksache 16/5048, S. 39.
[1832] BT-Drucksache 16/5048, S. 39.

Information zum Schutz von Urheberrechten eingesetzt wird, ausreicht. Dem Schutz personenbezogener Daten des vermeintlichen Rechtsverletzers wird folglich nach deutschem Recht eine höhere Bedeutung zugesprochen als nach US-amerikanischem Recht.

Anders sieht es jedoch hinsichtlich Verkehrsdaten aus. Während Urheberrechtsinhaber nach deutschem Recht einen Auskunftsanspruch nur unter Richtervorbehalt geltend machen können, bedarf es nach US-amerikanischem Recht sogar der Einleitung eines gerichtlichen Verfahrens, innerhalb dessen der Rechteinhaber dann einen entsprechenden Antrag auf Auskunft gegen den ISP stellen kann. Im Gegensatz zu einer *subpoena* im Rahmen des DMCA werden die Gerichte aber oftmals vor Erlass einer entsprechenden Anordnung die Begründetheit des geltend gemachten Anspruchs prüfen. Zudem können die Gerichte den Erlass der Anordnung an zusätzliche Kriterien knüpfen und so bspw. bestimmen, dass der ISP der Anordnung erst nachkommen darf, nachdem er eine Kopie der Anordnung sowie des Klageantrags an den vermeintlichen Rechtsverletzer weitergeleitet hat und der vermeintliche Rechtsverletzer innerhalb von 30 Tagen nach Erhalt der Anordnung keinen Antrag zur Aufhebung der Anordnung bei Gericht eingereicht hat.[1833]

4. Verantwortlichkeit ggü. Nutzer

Entfernt oder sperrt der ISP Informationen unter Beachtung der Bestimmungen des DMCA, so ist er hierfür gegenüber dem betroffenen Nutzer nicht zur Verantwortung zu ziehen.[1834] Hinsichtlich des Host-Providers ist zusätzlich auf die Beachtung der Bestimmungen zum *Notice and Takedown*-Verfahren abzustellen. Den ISP trifft folglich eine diesbezüglich umfassende

[1833] So bspw. in Malibu Media, LLC v. John Doe, CIVIL NO. JKB-15-2359 (D. Md. Aug 14, 2015). Ein entsprechender Antrag auf Aufhebung kann anonym gestellt werden, der vermeintliche Rechtsverletzer muss lediglich gegenüber dem Clerk des Gerichts seine Daten preisgeben.
[1834] Siehe hierzu S. 337.

Haftungsfreistellung gegenüber seinem Nutzer. Einzige Voraussetzung ist, dass der ISP in gutem Glauben gehandelt hat.

Im deutschen Recht ist die Haftungssituation des ISP gegenüber seinem Nutzer unklar. Grundsätzlich denkbar sind im Falle des Host-Providers sowohl vertragliche als auch gesetzliche Ansprüche des Nutzers, im Falle des Access-Providers vornehmlich gesetzliche Ansprüche.[1835] Der ISP ist im deutschen Recht somit einer erheblich höheren rechtlichen Unsicherheit ausgesetzt als im US-amerikanischen Recht. Denn auch wenn bislang keine Fälle hinsichtlich der Geltendmachung von Ansprüchen des Nutzers gegen den Host- oder Access-Provider bekannt sind, kann dies für die Zukunft nicht ausgeschlossen werden. Ansprüche des vermeintlichen Rechtsverletzers gegenüber dem Cache-Provider und dem Linksetzenden bzw. Suchmaschinenanbieter sind hingegen nicht ersichtlich.

II. Host-Provider

Prinzipiell sind die Anforderungen an den Host-Provider im deutschen und US-amerikanischen System ähnlich ausgestaltet. Den Host-Provider trifft in gleicher Weise eine Pflicht zur Entfernung bzw. Sperrung von urheberrechtsverletzenden Inhalten. Anders als im deutschen Recht wurde durch das *Notice and Takedown*-System jedoch ein formales Verfahren etabliert, welches maßgeblich zur Rechtssicherheit des Host-Providers beigetragen hat.

1. Aktiver ISP/right and ability to control

Nach der Rechtsprechung des EuGH fällt nur derjenige Host-Provider unter die Haftungsprivilegien, der seine Dienste neutral erbringt, das heißt rein technisch, automatisch und passiv, und der keine Kenntnis oder Kontrolle über die weitergeleitete oder gespeicherte Information besitzt.[1836] Sobald er eine aktive Rolle einnimmt, die ihm Kenntnis oder Kontrolle über die Inhalte verschafft, verliert er nach Auffassung des Gerichtshofs seine

[1835] Siehe hierzu S. 213.
[1836] Siehe hierzu S. 46.

Privilegierung hinsichtlich dieser Inhalte. Hierzu zähle bspw. eine Hilfestellung des Plattform-Betreibers in Form einer Optimierung der Präsentation der Verkaufsangebote sowie einer entsprechenden Bewerbung dieser Angebote, allerdings nur sofern ihm hierdurch eine Kenntnis oder Kontrolle der Inhalte zukomme.

Eine ähnliche Bestimmung findet sich in § 512 (c) (1) (B) DMCA, der das Recht und die Möglichkeit einer Kontrolle durch den Host-Provider im Zusammenhang mit einem finanziellen Vorteil als Ausschlusskriterium für die Inanspruchnahme des *safe harbor* festlegt. Eine entsprechende Kontrollmöglichkeit wurde in einem Fall bejaht, in dem der Host-Provider die Webseite eines Dritten vorab überprüfte und die Webseiten-Betreiber umfassend beriet.[1837] Von den Gerichten erwogen wurde zudem eine entsprechende Kontrolle in Fällen, in denen der Plattform-Betreiber aktiv in die Auflistung, die Versteigerung, den Verkauf und die Lieferung von von Dritten angebotenen Produkten involviert ist oder in denen der Host-Provider eine Vorabprüfung der Produkte vornimmt, eine Bearbeitung der Produktbeschreibung oder Preise für die Produkte vorschlägt.

Die Konstrukte des aktiven Providers des EuGH und des *right and ability to control* des DMCA sind auf den ersten Blick sehr ähnlich. Beide können Fälle umfassen, in denen der Host-Provider sich aktiv in die Gestaltung bzw. Optimierung von Verkaufsangeboten Dritter auf ihrer Plattform einbringt. Während im US-amerikanischen Recht jedoch eine grundsätzliche Kontrollmöglichkeit des Host-Providers auf die auf seiner Plattform durch die Nutzer bereitgestellten Inhalte als ausreichend erachtet wird, ist bei dem europäischen Pendant nach der hier vertretenen Auffassung nicht eine *generelle* Kontrollmöglichkeit ausreichend, sondern der Host-Provider muss eine Möglichkeit der Kontrolle des *spezifischen* Inhalts haben und verliert dann lediglich hinsichtlich *diesen* Inhaltes seine Privilegierung. Somit ist der Anwendungsbereich des europäischen Pendants wesentlich enger

[1837] Siehe hierzu S. 291.

gezogen. Dies ist vor dem Hintergrund auch interessengerecht, da der EuGH den aktiven Provider von einer Inanspruchnahme der Privilegien hinsichtlich des betroffenen Inhaltes ausschließt, während die Kontrollmöglichkeit des DMCA und die zusätzliche Voraussetzung des finanziellen Vorteils an einen Verlust des *safe harbor* geknüpft ist.

Sowohl der vom EuGH statuierte aktive Provider als auch die im DMCA genannte *right and ability to control* sind grundsätzlich dazu geeignet, Rechtsunsicherheit bei dem Host-Provider hinsichtlich seiner potentiellen Möglichkeit zur Inanspruchnahme der Privilegien zu begründen.

2. Informationen Dritter

Nach § 10 TMG sind Host-Provider für fremde Informationen privilegiert. § 512 (c) DMCA hingegen spricht von einer Speicherung des Materials *at the direction of a user*. Bei letzterem ist unbeachtlich, ob das Material nach dem Upload des Nutzers von Mitarbeitern des Host-Providers gesichtet oder überprüft wurde, es ist lediglich ausschlaggebend, dass der Nutzer den Upload ursprünglich initiiert hat.[1838] Anders ist es im deutschen Recht. Hier hat der BGH ein zu eigen Machen von ursprünglich von Dritten hochgeladenen Inhalten angenommen, sofern der Host-Provider die Inhalte vor Upload sichtet und nach objektiver Sicht auf Grundlage einer Gesamtbetrachtung nach außen sichtbar die inhaltliche Verantwortung für die Inhalte übernimmt.[1839] Ausschlaggebend war, dass der Host-Provider die Inhalte vor Veröffentlichung einer redaktionellen Kontrolle unterwarf und sich diese aus objektiver Sicht der Nutzer zu eigen mache.

Hingegen geht die ECRL von einem technischen Verständnis aus und stellt auf die durch den Nutzer eingegebenen Informationen ab. Das Konstrukt des zu eigen Machens ist dafür geeignet, den Host-Provider hinsichtlich der von ihm zu treffenden Maßnahmen, um einer Haftung zu entgehen, erheblich zu verunsichern. So muss er

[1838] Siehe hierzu S. 321.
[1839] Siehe hierzu S. 43.

befürchten, aufgrund von eigenen Kontrollmaßnahmen und entsprechender Einbindung von fremden Inhalten auf seiner Webseite einer Haftung ausgeliefert zu sein. Die genauen Konturen eines zu eigen Machens von Inhalten sind ungeklärt. Im US-amerikanischen Recht hingegen kommt es lediglich auf den ursprünglichen Initiator an. Der Host-Provider muss daher nicht aufgrund eigener Überprüfungsmaßnahmen um einen Verlust seiner Privilegierung fürchten. Dies trägt maßgeblich zu seiner Rechtssicherheit bei.

3. Kenntnis

Auslöser für die Pflicht zur Löschung bzw. Sperrung von Inhalten ist nach § 10 TMG die Kenntnis des Host-Providers. Erforderlich ist eine subjektive Kenntnis des spezifischen Inhalts, was eine Kenntnis der Rechtswidrigkeit des Inhaltes einschließt.[1840] Eine Unterscheidung gibt es jedoch hinsichtlich der Privilegierung vor Schadensersatzansprüchen. Hier kann der Host-Provider sich bereits nicht auf eine Privilegierung berufen, sofern ihm Tatsachen oder Umstände bekannt sind, aus denen eine rechtswidrige Handlung oder Information offensichtlich wird, folglich wird ein „Kennenmüssen“ bereits als ausreichend erachtet.[1841]

Eine fast identische Regelung enthalten § 512 (c) (1) (A) (i) und (ii) DMCA. Während für eine *actual knowledge* auch die subjektive Kenntnis des spezifisch urheberrechtsverletzenden Materials, inkl. einer Kenntnis der rechtsverletzenden Natur des Materials, vorausgesetzt wird, verlangt die *red flag knowledge* allerdings mehr als ein objektives Kennenmüssen.[1842] Der Host-Provider muss sich vielmehr subjektiv Tatsachen bewusst sein, die eine spezifische Rechtsverletzung für eine vernünftige Person objektiv offensichtlich gemacht hätte.

In Deutschland existiert kaum Rechtsprechung hinsichtlich der Erfordernisse für die Geltendmachung einer Kenntnis oder eines Kennenmüssens. Dies hat den Grund, dass die Rechtsprechung die

[1840] Siehe hierzu S. 52.
[1841] Siehe hierzu S. 53.
[1842] Siehe hierzu S. 269 und S. 272.

Privilegien in der Praxis, wo es sich hauptsächlich um die Geltendmachung von Unterlassungsansprüchen dreht, nicht anwendet, so dass auch die einzelnen Voraussetzungen bislang kaum geprüft wurden. Aus der spärlichen Rechtsprechung kann jedoch geschlossen werden, dass in der Praxis auf eine Kenntnis meist aus der Zusendung eines Hinweises bzw. einer Abmahnung durch den Rechteinhaber geschlossen wird. Bedauerlicherweise wird dies jedoch nicht weiter thematisiert. Es ist also unklar, welcher Inhalt eines solchen Hinweises als ausreichend erachtet wird, um dem Host-Provider eine Kenntnis zu vermitteln.

Der BGH hat in seinem „Stiftparfum"-Urteil hinsichtlich einer behaupteten Markenrechtsverletzung ausgeführt, dass der Hinweis so konkret gefasst sein muss, dass der Host-Provider den Rechtsverstoß unschwer, d.h. ohne eingehende rechtliche und tatsächliche Überprüfung, feststellen kann.[1843] Das genaue Ausmaß einer insoweit vom Host-Provider zu verlangenden Prüfung sei abhängig von den Umständen des Einzelfalls, insbesondere dem Gewicht der behaupteten Rechtsverletzung sowie der Erkenntnismöglichkeit des Host-Providers.[1844] Die Beibringung von Belegen hinsichtlich der behaupteten Rechtsverletzung, der Inhaberschaft an den Schutzrechten sowie der Berechtigung zur Rechtsverfolgung sah der Senat im vorliegenden Fall für nicht erforderlich an.[1845]

Er weist jedoch darauf hin, dass der Abgemahnte grundsätzlich nach Treu und Glauben dazu verpflichtet sei, den Abmahnenden auf berechtigte Zweifel an der Abmahnung hinzuweisen und ggf. nach angemessenen Belegen hinsichtlich der behaupteten Rechtsverletzung oder der Befugnis zur Verfolgung der Rechtsverletzung zu verlangen.[1846] Er bezieht sich hier jedoch auf § 12 UWG, welcher eine Abmahnung zur Geltendmachung eines Unterlassungsanspruches vor Einleitung eines gerichtlichen

[1843] BGH GRUR 2011, 1038, 1040.
[1844] BGH GRUR 2011, 1038, 1040 f.
[1845] BGH GRUR 2011, 1038, 1041.
[1846] BGH GRUR 2011, 1038, 1041.

Verfahrens voraussetzt. Es ist fraglich, ob diese Grundsätze für den Hinweis auf eine Rechtsverletzung herangezogen werden können. Bei der im vorliegenden Fall maßgeblichen Abmahnung handelte es sich nämlich insoweit um keine Abmahnung im Sinne des § 12 UWG, sondern um einen Hinweis des Rechteinhabers, welcher dem Host-Provider die für die Prüfpflichten erforderliche Kenntnis vermitteln soll.[1847] Es kann also durchaus bezweifelt werden, dass die für die im Wettbewerbsrecht geforderte vorgerichtliche Abmahnung aufgestellten Grundsätze auch für die eine Prüfpflicht begründende Kenntnis in Form des Hinweises Geltung beanspruchen können. Zudem wurde offen gelassen, ob ein für die Entstehung einer Prüfpflicht ausreichender Hinweis dann fehlt, wenn der Host-Provider wegen berechtigter Zweifel weitere Belege beim Rechteinhaber anfordert und dieser der Aufforderung nicht Folge leistet.[1848]

Die vom Senat aufgestellte einzelfallabhängige Bewertung des Hinweises birgt jedenfalls ein erhebliches Missbrauchspotential sowie Rechtsunsicherheit für den Host-Provider. Aufgrund fehlender expliziter Vorgaben, könnten die Host-Provider geneigt sein, Inhalte „auf Zuruf" zu löschen.

Im US-amerikanischen Recht hingegen scheint die *actual knowledge* und *red flag knowledge* aufgrund des gesetzlich stipulierten *Notice and Takedown*-Verfahrens[1849] eine lediglich untergeordnete Rolle zu spielen. Das Vorhandensein dieses Verfahrens verleitet Gerichte irrigerweise dazu, eine *actual knowledge* prinzipiell zu verneinen, sofern der Rechteinhaber vor Einleitung eines Verfahrens keine *notification* nach den Vorgaben des DMCA versendet hat. Auch wenn das Vorliegen einer *red flag knowledge* bereits des Öfteren durch die Rechteinhaber vorgetragen wurde, haben die Gerichte bislang meist eine entsprechende

[1847] So auch Holznagel, GRUR Int. 2014, 105, 109, der diesbzgl. ausführt, dass die Abmahnung dem Primärzweck dient, einen Streit ohne Prozess beizulegen, während es bei der Verdachtsmeldung darum geht, Prüfungspflichten auszulösen, deren Verletzung nachgelagert zu einer Haftung führen kann.
[1848] BGH GRUR 2011, 1038, 1041.
[1849] Siehe hierzu S. 296.

Kenntnis verneint. Lediglich in *Columbia v. Fung*, wo der Host-Provider seine Nutzer explizit zum hoch- und herunterladen spezifischer urheberrechtlich geschützter Werke ermutigt und umfangreiche Assistenz hinsichtlich des Auffindens urhebeberrechtlich geschützter Filme geleistet hat, wurde eine *red flag knowledge* aufgrund fehlender gegenteiliger Beweisführung hinsichtlich der streitgegenständlichen Werke durch den Host-Provider bejaht.[1850] Die genauen Konturen der *red flag knowledge* sind aber weitestgehend unbekannt und die Geltendmachung einer solchen birgt für beide Parteien eine hohe Unsicherheit. Soweit möglich, wird daher der Rechteinhaber regelmäßig auf die Versendung einer *notification* zurückgreifen.

Es bleibt zudem im deutschen Recht die, bislang kaum beleuchtete Frage, ob die Kenntnis i.S.d. § 10 S. 1 Nr. 1 TMG und die Kenntnis, welche im Rahmen der Störerhaftung die Prüfungspflichten auslöst, identisch sind. Diese Frage stellt sich allerdings nur für den Fall, dass noch immer von einer Unanwendbarkeit der Haftungsprivilegien des § 10 TMG auf Unterlassungsansprüche ausgegangen wird. Denn dann wäre für die Definition der Kenntnis nicht § 10 TMG maßgeblich, sondern der im Rahmen der Störerhaftung entwickelte Begriff der Kenntnis. Da mittlerweile jedoch davon auszugehen ist, dass der BGH auch die Unterlassungsansprüche grundsätzlich der Privilegierung des § 10 TMG unterwirft, kann diese Frage unbeantwortet bleiben.

Fälle von bewusstem Wegschauen des Host-Providers können in Deutschland unter die Umstandskenntnis fallen, in den USA unter die *red flag knowledge*. Entscheidend sind in beiden Rechtsordnungen die jeweiligen Umstände des Einzelfalls.

4. Förderung von Rechtsverletzungen

Abseits der Haftungsprivilegien hat der BGH zunächst im Rahmen der Haftung eines Vertreibers von Peer-to-Peer-Software geurteilt, dass diesen im Rahmen der Störerhaftung erhöhte Prüfpflichten treffen, sofern er mit einer rechtswidrigen

[1850] Siehe hierzu S. 272.

Verwendungsmöglichkeit der Software geworben hat.[1851] Er habe von einem weiteren Vertrieb abzusehen, solange die durch diese Werbung geschaffene Gefahr weiter bestehe. Diese Rechtsprechung wurde in der Folge vom selben Senat auf den Host-Provider übertragen, in dem Sinne, dass dieser, sofern er ein gefahrgeneigtes Geschäftsmodell betreibt in dem Sinne, dass dieses von vornherein auf Rechtsverletzungen angelegt ist oder er durch eigene Maßnahmen die Gefahr einer rechtswidrigen Nutzung erhöht, diese Gefahr auszuräumen habe. Es ist unklar, ob und wann den Host-Provider demzufolge Prüfpflichten bereits vor einer spezifischen Kenntnis treffen und welchen genauen Umfang diese Pflichten haben.[1852] Jedenfalls treffen denjenigen, der die rechtsverletzende Nutzung des Dienstes in irgendeiner Weise fördert, erhöhte Prüfungspflichten.

Entsprechend hat auch die US-amerikanische Rechtsprechung eine Haftung für die Förderung von Rechtsverletzungen seitens des ISP im Rahmen des *common law* anerkannt.[1853] Nach Auffassung des *Ninth Circuit* kann jedoch auch derjenige Host-Provider, der nach common law wegen *inducement* haftet, von den Privilegien des DMCA erfasst sein. Die Privilegien seien nicht von Natur aus inkompatibel mit einer potentiellen *inducement liability*.

Die Behandlung von Host-Providern, die rechtsverletzende Tätigkeiten ihrer Nutzer fördern, ist in Deutschland und den USA bislang sehr ähnlich. In beiden Ländern dürften diese Host-Provider zunächst grundsätzlich in den Anwendungsbereich der *safe harbor*-Privilegien fallen, sofern sie dessen Voraussetzungen erfüllen. Allerdings gilt dies momentan nach der deutschen Rechtsprechungspraxis nicht für Unterlassungsansprüche. Entsprechend werden dem gefahrgeneigten Host-Provider von der Rechtsprechung bislang sehr umfangreiche Prüfpflichten auferlegt, nachdem er Kenntnis über eine spezifische Rechtsverletzung erlangt hat. Von Bedeutung sind die Privilegien daher nur für die

[1851] BGH GRUR 2009, 841, 843.
[1852] Siehe hierzu S. 131.
[1853] Siehe hierzu S. 241.

Geltendmachung von Schadensersatzansprüchen gegen den Host-Provider. Hier kann dem Host-Provider ein Schutz des § 10 TMG nur verwehrt werden, sofern ihm Tatsachen oder Umstände bekannt sind, aus denen eine rechtswidrige Handlung oder Information offensichtlich wird. Ob dies bei demjenigen Host-Provider, welcher aktiv Rechtsverletzungen innerhalb seines Dienstes fördert, gegeben ist, wird im jeweiligen Einzelfall zu prüfen sein.

In den USA hingegen wird in der Praxis eine Inanspruchnahme des *safe harbor*-Privilegs an dem finanziellen Vorteil und der Kontrollmöglichkeit des Host-Providers regelmäßig scheitern.[1854]

5. Take-Down v. Stay-Down

Während die USA über ein gesetzlich detailliert geregeltes *Notice and Takedown*-System verfügen, kann man das durch die deutsche Rechtsprechung entwickelte Konzept als sog. *Notice and Stay-down*-System bezeichnen. Korrekterweise müsste dies eigentlich *knowledge and stay down* genannt werden, da eben ein Hinweis des Urhebers nach deutschem Recht nicht erforderlich ist, sondern es vielmehr auf die, wie auch immer erlangte, Kenntnis des Host-Providers ankommt. Denn nachdem der Host-Provider Kenntnis über eine spezifische Rechtsverletzung erlangt hat - in der Praxis geschieht dies meist durch Zusendung eines entsprechenden Hinweises des Rechteinhabers - steht der Host-Provider in der Pflicht, zukünftige kerngleiche Rechtsverletzungen durch ihn treffende Prüfpflichten zu verhindern. Im Endeffekt bedeutet dies eine umfassende Filterung des Datenverkehrs.[1855]

Nachfolgend werden die wichtigsten Aspekte der beiden Verfahren gegenübergestellt und bewertet.

[1854] So auch in Columbia Pictures Industries, Inc. v. Fung, 710 F.3d 1020, 1044 ff. (9th Cir. 2013).

[1855] Zutreffend daher Harmon: *„Notice-and-Stay-Down" Is Really „Filter-Everything"*.

a) Notice v. Kenntnis

Auch wenn der Host-Provider nach § 512 (c) (1) (A) DMCA zum *takedown* verpflichtet ist, nachdem er *actual* oder *red flag knowledge* über eine spezifische Rechtsverletzung erlangt hat, ist dieser *takedown* auf Grundlage von Kenntnis nicht Teil des *Notice and Takedown*-Verfahrens, welches in § 512 (c) (1) (C) DMCA geregelt ist und für welches entsprechend auch das gesetzlich festgeschriebene *put back*-Verfahren Anwendung findet.

Im Gegensatz hierzu basiert das deutsche *stay down*-System nach seinem gesetzlichem Wortlaut auf einer Kenntnis bzw. einem Kennenmüssen des Host-Providers hinsichtlich einer spezifischen Rechtsverletzung. Während es also im deutschen Recht entweder auf die positive Kenntnis eines urheberrechtsverletzenden Inhaltes oder im Fall von Schadensersatzansprüchen auf ein Kennenmüssen eines solchen urheberrechtlichen Inhalts ankommt, reicht es für das US-amerikanische *takedown*-Verfahren aus, wenn die formalen Voraussetzungen an die *notification* erfüllt sind.

Die Vorteile des US-amerikanischen *Notice and Takedown*-Verfahrens liegen auf der Hand. Der Host-Provider bekommt durch die detaillierten gesetzlichen Vorgaben die an eine *notification* gestellt werden, die nötige Rechtssicherheit. Er weiß i.d.R. genau, wann eine *notification* den gesetzlichen Anforderungen entspricht und wann nicht und kann sich bei Einhalten der weiteren gesetzlichen Handlungsanweisung auf seine Privilegierung sowohl im Hinblick auf den Urheberrechtsinhaber als auch im Hinblick auf den Inhalteanbieter verlassen.

Dahingegen ist die Bestimmung einer Kenntnis des urheberrechtsverletzenden Materials i.S.d. § 10 TMG nicht so eindeutig. Handelt es sich beispielsweise bei dem beanstandeten Material um einen Musik-Remix oder eine Film-Parodie, kann eine Beurteilung durchaus problematisch sein und erfordert eine gewisse rechtliche Expertise.[1856] In der Praxis spielt dies bislang

[1856] Selbst für Urheberrechtsexperten ist eine eindeutige Aussage, ob ein bestimmtes Werk als Urheberrechtsverletzung einzustufen ist oder bspw. als selbstständiges Werk eine freie Benutzung darstellt und daher keiner

jedoch keine nennenswerte Rolle, da hier dem Host-Provider regelmäßig eine Kenntnis aufgrund vorhergehenden Hinweises des Rechteinhabers zugeschrieben wird. Da das deutsche Recht allerdings keine expliziten Vorgaben hinsichtlich eines solchen Hinweises enthält, kann dies in der Praxis dazu führen, dass Inhalte vorschnell gelöscht werden.

Zwar birgt auch das US-amerikanische Verfahren aufgrund des fehlenden Erfordernisses einer materiell-rechtlichen Prüfung diese Gefahr, hier gibt § 512 (c) (3) DMCA jedoch wenigstens gewisse inhaltliche Mindestanforderungen an die *notification* vor, die sowohl den Host-Provider als auch dem einer Urheberrechtsverletzung Bezichtigten zugutekommen sollen. Zum einen soll hierdurch sichergestellt werden, dass der Host-Provider das beanstandete Material durch Angabe genauer Informationen zur Lokalisierung des Materials ohne weiteren Aufwand auffinden kann, zum anderen soll der Inhalteanbieter dadurch geschützt werden, dass der Absender der *notification* seine Ermächtigung zur Wahrnehmung der Urheberrechte eidesstattlich zu versichern sowie eine Erklärung hinsichtlich seines guten Glaubens bzgl. der Verletzung seiner Rechte abzugeben hat. Zudem wird die Angabe weiterer Informationen über den Absender der *notification* zur Kontaktaufnahme durch den Host-Provider verlangt. Der Host-Provider wird folglich von der Last einer Beurteilung der erhaltenen *notification* befreit und erlangt dahingehend auch mehr Rechtssicherheit für sein weiteres Handeln.

b) Benachrichtigung des Nutzers

Um einer potentiellen Haftung für die Löschung bzw. Sperrung des Materials gegenüber seinem Nutzer zu entgehen, hat der Host-Provider diesen nach US-amerikanischem Recht über die Löschung bzw. Sperrung zu informieren.[1857] Eine entsprechende Pflicht bzw. eine Obliegenheit zur Benachrichtigung des Nutzers ist im deutschen Recht nicht speziell geregelt.

Zustimmung des Urhebers bedarf oder der Schranke des Zitats unterliegt, oft schwierig.

[1857] Siehe hierzu S. 309.

Eine entsprechende Pflicht ließe sich allenfalls im Innenverhältnis aus § 241 Abs. 2 BGB herleiten, welcher die Vertragsparteien jeweils zur Rücksicht auf die Rechte, Rechtsgüter und Interessen des anderen Vertragspartners verpflichtet.[1858]

Das US-amerikanische Recht ist in dieser Hinsicht für den Nutzer von Vorteil. Demgegenüber werden nach deutscher Rechtslage für eine entsprechende freiwillige Benachrichtigung des Nutzers durch den Host-Provider lediglich Gründe der Erhaltung der Vertragsbeziehung bzw. Kundenzufriedenheit sprechen.

Folglich hat der Host-Provider im US-amerikanischen Recht durch die drohende potentielle Haftung gegenüber dem Nutzer einen erhöhten Anreiz zur Benachrichtigung des Nutzers, was den Interessen des Nutzers zu Gute kommt.

c) Verteidigungsmöglichkeiten des betroffenen Nutzers

Der durch die Entfernung bzw. Sperrung betroffene Nutzer hat nach US-amerikanischem Recht die Möglichkeit, sich durch die Versendung einer *counter notification* gegen die behauptete Rechtsverletzung zu verteidigen.[1859] Eine entsprechend gesetzlich festgeschriebene Verteidigungsmöglichkeit des Nutzers fehlt im deutschen Recht. Entfernt bzw. sperrt der Host-Provider Inhalte des Nutzers, ist er nach den Bestimmungen des § 10 TMG bzw. den Grundsätzen der Störerhaftung gegenüber dem Rechteinhaber privilegiert, sofern er seinen Prüfpflichten nachkommt. Zwar steht es dem Nutzer insoweit offen, eine Mitteilung hinsichtlich zu Unrecht entfernter Inhalte an den Host-Provider zu machen, es besteht insofern allerdings kein haftungsbezogener Anreiz für den Host-Provider, auf die Mitteilung zu reagieren. Einzig vertragsbezogene Gesichtspunkte im Sinne einer Kundenzufriedenheit oder allgemeine Image-Aspekte könnten den Host-Provider dazu veranlassen, eine entsprechende Mitteilung nicht unbeantwortet zu lassen. Im Gegensatz hierzu schafft das US-amerikanische Recht durch die Zuweisung des *safe harbors* einen

[1858] So Holznagel, GRUR Int. 2014, 105, 111.
[1859] Siehe hierzu S. 333.

großen Anreiz zur Beachtung der *counter notification* und des damit einhergehenden *put back*-Verfahrens.

d) Put back-Verfahren

Hinsichtlich der Vorgehensweise nach Erhalt einer *counter notification* durch den Nutzer enthält das US-amerikanische Recht gesetzlich detaillierte Bestimmungen.[1860] So hat der Host-Provider dem Absender der *notification* umgehend eine Kopie der *counter notification* zukommen zu lassen und ihn darüber zu informieren, dass das beanstandete Material in 10 Tagen wieder eingestellt bzw. entsperrt wird. Anschließend ist das Material in nicht weniger als 10 und nicht mehr als 14 Werktagen nach Erhalt der *counter notification* wieder zugänglich zu machen, es sei denn, der Rechteinhaber reicht innerhalb dieses Zeitraums Klage gegen den Absender der *counter notification* ein.

Dem Nutzer wird hier folglich eine einfache Möglichkeit geboten, das Material durch den Host-Provider wieder zugänglich machen zu lassen und sich so gegen die *notification* und die damit einhergehend behauptete Rechtsverletzung zu wehren. Für den Host-Provider bedeutet dies Rechtssicherheit, solange er sich an die gesetzlich vorgeschriebenen Regelungen hält.

Fraglich ist allerdings, warum die Weiterleitung einer Kopie der *counter notification* gesetzlich vorgeschrieben wurde. Da die *counter notification* u.a. Name, Adresse und Telefonnummer des Inhalteanbieters enthält, wird er hierdurch letztendlich seiner Anonymität beraubt, ohne dass es hierfür einer Glaubhaftmachung der Begründetheit der beanstandeten Rechtsverletzung seitens des Rechteinhabers bedarf. Der Nutzer hat folglich für die Verteidigung seiner Rechte im Gegenzug seine Anonymität aufzugeben. Der Rechteinhaber wird damit in die Lage versetzt, ein gerichtliches Verfahren direkt gegen den Rechtsverletzer einzuleiten und muss nicht auf die Einreichung einer John Doe-Klage zurückgreifen.

[1860] Siehe hierzu S. 336.

Aufgrund der fehlenden Verteidigungsmöglichkeit im TMG, gibt es entsprechend auch keine Bestimmungen hinsichtlich einer Obliegenheit zur Wiedereinstellung bzw. Entsperrung eines aufgrund einer *notification* entfernten oder gesperrten Inhaltes.

Dem Host-Provider bleibt es jedoch unbenommen, das Material nach einer entsprechenden Mitteilung auf freiwilliger Basis wieder einzustellen oder freizuschalten. Ob er sich für ein solch freiwilliges *put back* entscheidet, ist allerdings fraglich. Es besteht hierdurch die Gefahr, dass der Host-Provider durch eine entsprechende Wiedereinstellung bzw. Freischaltung seine Privilegierung verliert und ggü. dem Rechteinhaber unterlassungs- oder schadensersatzpflichtig wird. Zwar besteht für den Fall einer Unterlassung des *put back* auch die Gefahr einer Haftung ggü. dem Nutzer, diese Gefahr ist aber eher überschaubar.[1861] Der Host-Provider wird in Deutschland daher im Zweifel darauf verzichten, nach Mitteilung durch den Nutzer, dass die Löschung und Entfernung eines bestimmten Inhaltes unrechtmäßig erfolgte, diesen wieder einzustellen. Der Nutzer hat somit keine ausreichende Möglichkeit sich gegen unberechtigte *takedowns* zu verteidigen. Ihm wird hier oftmals nur die gerichtliche Geltendmachung seiner Ansprüche übrig bleiben. Dies ist insbesondere kritisch zu sehen im Hinblick auf die Informationsfreiheit der Internetnutzer.

Unter diesem Gesichtspunkt wird auch das US-amerikanische *put back*-Verfahren kritisiert. Denn auch bei umgehender *counter notification* ist das Material zunächst für 10-14 Tage nicht abrufbar. Je nach Art des Materials kann sich dieser Zeitraum als entscheidend für den Inhalteanbieter darstellen.[1862]

e) Haftung gegenüber dem Nutzer

Entfernt der Host-Provider das Material aufgrund *actual knowledge*, *red flag knowledge* oder einer *notification* in gutem Glauben, ist er vor etwaigen Ansprüchen des Inhalteanbieters

[1861] Siehe hierzu S. 213.
[1862] Siehe hierzu S. 336.

geschützt.[1863] Bei einer aufgrund einer *notification* durchgeführten Entfernung oder Sperrung des Materials hat der Host-Provider zusätzlich die gesetzlich vorgeschriebenen Regelungen des *Notice and Takedown*-Verfahrens zu beachten. Eine Haftungsprivilegierung kommt dem Host-Provider damit nicht lediglich gegenüber dem Rechteinhaber zugute sondern auch gegenüber dem betroffenen Nutzer. Dies ist vor dem Hintergrund eines der Ziele des DMCA, nämlich der Schaffung von Rechtssicherheit für den Host-Provider, durchaus konsequent.

In Deutschland hingegen greifen die Privilegien des TMG lediglich gegenüber dem Rechteinhaber. Im Hinblick auf potentielle Ansprüche seiner Nutzer steht der Host-Provider „schutzlos" dar. Es kann bezweifelt werden, dass dies der Schaffung von Rechtssicherheit zweckdienlich ist. Zwar kann sich die Geltendmachung von Ansprüchen durch den Nutzer aufgrund einer schuldhaften vertraglichen Pflichtverletzung oder der Verletzung eines sonstigen Rechts des Host-Providers in der Praxis als schwierig erweisen.[1864] Die hiermit verbundenen Unsicherheiten werden den Nutzer eher davor zurückschrecken lassen, Ansprüche gegen den Host-Provider aufgrund unberechtigter Entfernung oder Sperrung seiner Inhalte geltend zu machen. Dennoch ist die potentielle Möglichkeit der Geltendmachung entsprechender Ansprüche dazu geeignet, seitens des Host-Providers Unsicherheiten hinsichtlich der Art und des Umfangs einer etwaigen Haftung zu schüren.

f) Haftung für falsche Darstellung

Das US-amerikanische Recht setzt eine explizite Haftung für wissentlich falsche Angaben hinsichtlich der urheberrechtsverletzenden Natur eines bestimmten Materials oder der Rechtmäßigkeit eines bestimmten Materials fest.[1865] Nach dieser Bestimmung können entsprechend vorsätzlich gemachte falsche Angaben innerhalb der *notification* bzw. *counter notification* zu

[1863] Siehe hierzu S. 337.
[1864] Siehe hierzu S. 213.
[1865] Siehe hierzu S. 338.

Schadensersatzansprüchen auf Seiten des behaupteten Rechtsverletzers, des Urheberrechtsinhabers und des durch diese falsche Angabe betroffenen Host-Providers führen. Durch diese Bestimmung wird das notwendige Gleichgewicht zu dem gesetzlich zugewiesenen Vertrauensvorschuss hinsichtlich der materiell-rechtlichen Begründetheit des in der formal korrekten *notification* bzw. *counter notification* aufgeführten Anspruchs hergestellt. Da der Host-Provider das streitgegenständliche Material ohne weitergehende Prüfung nach Erhalt der formal korrekten *notification* entfernt bzw. sperrt und entsprechend ohne weitergehende Prüfung das Material nach Erhalt der *counter notification* wieder zugänglich macht, birgt dieses gesetzliche System eine vergleichsweise hohe Gefahr des Missbrauchs. Um potentielle Missbräuche durch arglistige Akteure abzuschrecken, wird durch § 512 (f) DMCA ausdrücklich klargestellt, dass hierdurch Schadensersatzansprüche auf diese zukommen können. Eine solch vorsätzliche *misrepresentation* liegt i.d.R. nicht vor, sofern der Host-Provider in gutem Glauben gehandelt hat. Bedenklich ist insoweit die teils durch die Gerichte vorgenommene weite Auslegung des Begriffs des guten Glaubens.[1866] Diese könnte die Haftung aufgrund wissentlicher und wesentlicher falscher Angaben faktisch entwerten.

Aufgrund fehlender gesetzlicher *Notice and Takedown*-Bestimmungen fehlt es im deutschen Recht auch an einer spezifischen Regelung hinsichtlich falscher Angaben des Urheberrechtsinhabers oder des vermeintlichen Rechtsverletzers gegenüber dem Host-Provider.

aa) Ansprüche Host-Provider gegen Urheberrechtsinhaber

Denkbar sind zunächst Ansprüche des Host-Providers gegen den Urheberrechtsinhaber aufgrund falscher Angaben in dem Hinweis, den er dem Host-Provider zugesendet hat. Nach der Rechtsprechung des BGH können unberechtigte Schutzrechtsverwarnungen einen Eingriff in das Recht am

[1866] Siehe hierzu S. 306.

eingerichteten und ausgeübten Gewerbebetrieb darstellen und entsprechend sowohl Unterlassungs- als auch Schadensersatzansprüche nach §§ 823 Abs. 1, 1004 BGB begründen.[1867] Einen entsprechenden Anspruch aufgrund eines unberechtigten Hinweises hat der I. Zivilsenat allerdings ohne weitergehende Begründung abgelehnt.[1868] Nach seiner Auffassung sei eine entsprechende Anwendung dieser Grundsätze auf Hinweise hinsichtlich behaupteter Rechtsverletzungen nicht geboten, da diese nicht die Qualität einer Schutzrechtsverwarnung[1869] hätten und somit auch nicht in das Recht des Host-Providers am eingerichteten und ausgeübten Gewerbebetriebes eingriffen.[1870] Es ist daher davon auszugehen, dass dem Host-Provider nicht die Möglichkeit offen steht, Schadensersatz- oder Unterlassungsansprüche gegen den Urheberrechtsinhaber geltend zu machen.[1871]

bb) Ansprüche vermeintlicher Rechtsverletzer gegen Urheberrechtsinhaber

Aufgrund der direkten Betroffenheit des Nutzers in Folge eines Hinweises über eine vermeintliche Rechtsverletzung an den Host-Provider erscheint es interessengerecht, im Falle eines falschen Hinweises entsprechende Entschädigungs- und Unterlassungsansprüche des Nutzers gegenüber dem Urheberrechtsinhaber anzuerkennen.

(1) Negative Feststellungsklage

Zunächst wäre grundsätzlich eine negative Feststellungsklage gem. § 256 ZPO seitens des Nutzers denkbar.[1872] Danach kann auf Feststellung des Bestehens oder Nichtbestehens eines Rechtsverhältnisses Klage erhoben werden, wenn der Kläger ein

[1867] BGH GRUR 2006, 433, 434 f.; BGH GRUR 2005, 882, 884 m.w.N.
[1868] BGH GRUR 2011, 152, 157.
[1869] Bei der Schutzrechtsverwarnung handelt es sich um eine ernstliche und endgültige Aufforderung zur Abgabe einer strafbewehrten Unterlassungserklärung, mit der sich der Abgemahnte verpflichtet die Urheberrechtsverletzung künftig zu unterlassen, siehe Glossner in Leupold/Glossner, Teil 2, Rn. 534.
[1870] BGH GRUR 2011, 152, 157.
[1871] A.A. Holznagel, S. 206, aufgrund des schwerwiegenden Eingriffs einer unberechtigten Verdachtsmeldung.
[1872] So auch Holznagel, S. 171.

rechtliches Interesse daran hat, dass das Rechtsverhältnis durch richterliche Entscheidung alsbald festgestellt wird.

Der Begriff des Rechtsverhältnisses umfasst auch Rechte aus absoluten Rechten, wie bspw. Urheberrechte.[1873] Der Nutzer wird hier i.d.R. ein rechtliches Interesse an der Feststellung haben, dass sein Inhalt keine Urheberrechte verletzt, da es sein Inhalt ist, der von dem Host-Provider aufgrund des Hinweises des Urheberrechtsinhabers entfernt wurde. Voraussetzung hierfür ist eine Berühmung oder Abmahnung des Urhebers, dass eine bestimmte Handlung seine Rechte verletzt.[1874] Eine solche Berühmung dürfte regelmäßig der von dem Urheberrechtsinhaber an den Host-Provider gesendete Hinweis hinsichtlich der behaupteten Rechtsverletzung darstellen. Unerheblich ist insofern, dass der Hinweis an den Host-Provider gesendet und damit die Geltendmachung der Urheberrechtsverletzung diesem gegenüber angezeigt wurde und nicht gegenüber dem Nutzer.[1875]

(2) Analoge Anwendung der Grundsätze der Abnehmerverwarnung

Denkbar wäre auch eine Übertragung der Grundsätze der ungerechtfertigten Schutzrechtsverwarnung in Form einer Abnehmerverwarnung.[1876] Bei der Abnehmerverwarnung, das heißt einer Abmahnung gegenüber dem Vertriebsvermittler, ist höchstrichterlich anerkannt, dass eine solch unberechtigte Abmahnung Unterlassungs- sowie bei Verschulden Schadensersatzansprüche des vermeintlichen Rechtsverletzers begründen kann wegen Eingriffs in das Recht des eingerichteten und ausgeübten Gewerbebetriebs als sonstiges Recht i.S.d. § 823 Abs. 1 BGB.[1877]

[1873] Rojahn in Loewenheim, § 94 Rn. 36.
[1874] Rojahn in Loewenheim, § 94 Rn. 36.
[1875] Siehe allgemein zu einem Feststellungsinteresse aufgrund von Rechtsverhältnissen zu Dritten oder zwischen Dritten: Foerste in Musielak/Voit, ZPO, § 256 Rn. 5.
[1876] So auch Holznagel, S. 182.
[1877] Siehe Glossner in Leupold/Glossner, Teil 2, Rn. 538.

Voraussetzung für die Geltendmachung dieses Eingriffs ist ein mit der Schutzrechtsverwarnung verbundenes ernsthaftes und endgültiges Unterlassungsverlangen. Auch wenn der Hinweis an den Host-Provider noch kein endgültiges Unterlassungsverlangen darstellt, so wird dieser Hinweis in der Praxis zumeist dazu führen, dass der Host-Provider den beanstandeten Inhalt entfernt und die ihn im Rahmen der Störerhaftung nun treffenden Prüfpflichten erfüllt, d.h. er Vorsorge treffen wird, dass kerngleiche Inhalte nicht mehr eingestellt werden. In der Praxis kommt dem Hinweis daher eine dem ernsthaften und endgültigen Unterlassungsverlangen vergleichbare Wirkung zu.[1878]

Fraglich ist, ob diese Grundsätze auch auf private Personen übertragen werden können. *Holznagel* sieht hier eine sachgerechte Fortbildung als geboten an, so dass nicht nur Eingriffe in den Gewerbebetrieb, sondern auch Verletzungen des Allgemeinen Persönlichkeitsrechts erfasst werden.[1879] Er sieht einen Eingriff in den von ihm neu konstruierten Schutzbereich der kommunikativen Entfaltung des Inhalteanbieters.[1880]

Sofern man eine Übertragbarkeit der Grundsätze der Abnehmerverwarnung auf Privatpersonen annimmt, scheint jedoch eine Bezugnahme auf das Recht auf Integrität und Vertraulichkeit informationstechnischer Systeme als sonstiges Recht[1881] zielführender.

cc) Ansprüche gegen den vermeintlichen Rechtsverletzer

Eine Inanspruchnahme des Nutzers wegen falscher Angaben im Hinblick auf die Reaktion eines *takedown* scheint sowohl von Seite des Urheberrechtsinhabers als auch des Host-Providers als unwahrscheinlich. Zum einen besteht insoweit schon keine gesetzliche Obliegenheit des Host-Providers zur Wiedereinstellung des Inhaltes. Er kann zwar im Innenverhältnis gegenüber dem Nutzer haften, wird dies jedoch vor dem Hintergrund des Verlusts

[1878] Im Ergebnis auch Holznagel, S. 180.
[1879] Holznagel, GRUR Int. 2014, 105, 112.
[1880] Holznagel, S. 198.
[1881] Siehe hierzu S. 218.

der Haftungsprivilegierung gegenüber dem Urheberrechtsinhaber im Zweifel hinnehmen und von einer Wiedereinstellung des Inhalts absehen.

Auch ein Anspruch des Urheberrechtsinhabers gegen den Inhalteanbieter aufgrund falscher Angaben gegenüber dem Host-Provider ist nicht offensichtlich. Für den Fall, dass der Inhalteanbieter dem Host-Provider mitteilt, dass die in dem Hinweis gemachten Angaben unwahr seien und der Host-Provider daraufhin das Material wieder online stellt, bleibt es dem Urheber ohnehin unbenommen, seine Rechte gegen den Inhalteanbieter gerichtlich geltend zu machen.

dd) Ergebnis

Das Fehlen expliziter gesetzlich festgelegter Haftungsregelungen im deutschen Recht führt dazu, dass der Host-Provider keine ersichtlichen Ansprüche gegen denjenigen hat, der ihm gegenüber falsche Angaben hinsichtlich einer Urheberrechtsverletzung macht. Auch die Geltendmachung von Rechten des vermeintlichen Rechtsverletzers ist mit Unsicherheiten belastet. Die unsichere Rechtslage wird den Nutzer daher im Zweifel davor abhalten, seine Rechte weiter zu verfolgen. Im Gegensatz hierzu sieht das US-amerikanische Recht explizite Haftungsregelungen für falsche Angaben des Rechteinhabers sowie des vermeintlichen Rechtsverletzers vor, was zu mehr Rechtssicherheit für alle Beteiligten sorgt.

g) Exkurs: Notice and Evaluation-Verfahren des BGH hinsichtlich Persönlichkeitsrechtsverletzungen

Im Hinblick auf die Haftung eines Host-Providers für persönlichkeitsrechtsverletzende Inhalte hat der VI. Zivilsenat in seiner „*Blog*“-Entscheidung ein von dem Host-Provider einzuhaltendes Verfahren aufgestellt und präzisiert, anhand dessen seine etwaige Verpflichtung zur Löschung des beanstandeten Materials zu messen sei.[1882]

[1882] BGH MMR 2012, 124, 126.

So soll der Host-Provider, nachdem er einen ausreichend konkreten Hinweis über eine Persönlichkeitsrechtsverletzung erhalten hat, diesen zunächst dem für den Blog Verantwortlichen zur Stellungnahme weiterleiten.[1883] Sofern innerhalb einer nach den Umständen angemessenen Frist eine Stellungnahme ausbleibt, könne von der Berechtigung der Beanstandung ausgegangen werden und der beanstandete Beitrag gelöscht werden.[1884] Stelle der für den Blog Verantwortliche die Beanstandung jedoch substanziiert in Abrede und ergäben sich daher an der Berechtigung der Beanstandung berechtigte Zweifel, solle der Host-Provider dies dem Betroffenen mitteilen und ggf. Nachweise verlangen aus denen sich die behauptete Rechtsverletzung ergibt.[1885] Sofern eine Stellungnahme des Betroffenen ausbleibe bzw. er die geforderten Nachweise nicht vorlege, habe der Host-Provider keine weitere Prüfung vorzunehmen.[1886] Ergäbe sich allerdings aus der Stellungnahme des Betroffenen bzw. den von ihm eingereichten Belegen auch unter Berücksichtigung einer etwaigen Äußerung des für den Blog Verantwortlichen eine rechtswidrige Verletzung des Persönlichkeitsrechts, habe der Host-Provider den beanstandeten Eintrag zu löschen.[1887]

In dem vom VI. Zivilsenat aufgestellten Verfahren wird teils irrigerweise das Pendant zu dem US-amerikanischen *Notice and Takedown*-Verfahren gesehen.[1888] Dies ist allerdings vor dem Hintergrund, dass das US-amerikanische System gerade nicht nach der materiell-rechtlichen Grundlage eines behaupteten Anspruchs fragt und keine dahingehende Beurteilung des Host-Providers gefordert wird, verfehlt. Aufgrund der hiermit verbundenen Rechtsunsicherheit sowie der zugewiesenen Richterrolle des Host-

[1883] BGH MMR 2012, 124, 126.
[1884] BGH MMR 2012, 124, 126.
[1885] BGH MMR 2012, 124, 126.
[1886] BGH MMR 2012, 124, 126.
[1887] BGH MMR 2012, 124, 126.
[1888] So bspw. Hoeren, MMR 2012, 127, 127; *Leupold* in Leupold/Glossner, Teil 2 Rn. 667.

Providers wurde dieses vom BGH aufgestellte Verfahren im Schrifttum zu Recht kritisiert.[1889]

Eine Übertragung dieses Verfahrens auf urheberrechtliche Streitigkeiten ist jedoch unwahrscheinlich. So lag diesem von dem BGH aufgestelltem Verfahren die Überlegung zu Grunde, dass Persönlichkeitsrechtsverletzungen sich oftmals nicht ohne Weiteres feststellen lassen, sondern es vielmehr einer Abwägung zwischen den Rechten des Betroffenen auf Schutz seiner Persönlichkeit sowie Achtung seines Privatlebens und dem geschützten Recht der Meinungs- und Medienfreiheit bedarf.[1890] Einer solchen Abwägung bedarf es aber bei Urheberrechtsverletzungen i.d.R. nicht, weshalb eine Übertragung unwahrscheinlich ist.[1891]

Denkbar wäre allenfalls eine richterliche Fortentwicklung und Übertragung dieses Verfahrens des Presserechts auf das Urheberrecht in dem Sinne, dass auch bei behaupteten Urheberrechtsverletzungen der Nutzer über die behauptete Rechtsverletzung informiert wird und ihm die Möglichkeit eingeräumt wird, sich gegen die Behauptung zur Wehr zu setzen.[1892] Nach derzeitiger Rechtslage wird dem Nutzer jedoch kein (gesetzliches) Recht eingeräumt, sich gegen eine Löschung bzw. Sperrung seiner Inhalte gegenüber dem Host-Provider zu verteidigen.

III. Cache-Provider

Obgleich die US-amerikanische Regelung hinsichtlich der Privilegierung des Cache-Providers auf den ersten Blick um einiges umfangreicher bzw. ausführlicher erscheint, so sind die gesetzlichen Bestimmungen des TMG hiermit nahezu identisch. Der Cache-Provider ist privilegiert, sofern er das Material nicht

[1889] So bspw. Holznagel, BGH, GRUR Int 2014, 105, 108; Rühl, LMK 2012, 338417, die auf die große Rechtsunsicherheit sowie die deutliche Mehrbelastung der Host-Provider hinweist. Zu kurz gedacht hingegen Dietrich, NJ 2012, 200, 201, der dem Host-Provider im Rahmen dieses Verfahrens lediglich eine Moderationsfunktion zukommen lassen will.
[1890] BGH MMR 2012, 124, 126.
[1891] So auch Hoeren, MMR 2012, 127, 127.
[1892] Ähnlich einer *counter notification* im US-amerikanischen Recht.

verändert, etwaige Bedingungen für den Zugang zu dem Material sowie etwaige Vorgaben hinsichtlich der Aktualisierung des Materials beachtet, die Sammlung von bestimmten Daten über die Nutzung des Materials nicht beeinträchtigt und er nach Kenntnis der Rechtswidrigkeit sowie Entfernung am Ursprungsort das Material entfernt bzw. sperrt.

Sowohl in den USA als auch in Deutschland findet der Cache-Provider wenig Beachtung in der Rechtsprechung sowie im öffentlichen Diskurs.

Klassischer Anwendungsfall für die Privilegien des Cache-Providers ist das Usenet, jedenfalls soweit es sich um Informationen handelt, die nicht auf dem eigenen Newsserver sondern auf dem Newsserver eines Dritten gespeichert sind und die der Usenet-Provider entsprechend auf Anfrage anderer Nutzer übermittelt.[1893]

Von US-amerikanischen Gerichten wurde diese Tätigkeit, allerdings noch vor Umsetzung des DMCA, dem Access-Provider zugeordnet.[1894] Seitdem behandelte soweit ersichtlich nur ein Fall die Privilegierung des Cache-Providers, allerdings erweist sich hier eine Einordnung der Cache-Funktion Googles als unzutreffend.[1895]

Auch unter den Voraussetzungen des § 9 TMG ist eine entsprechende Einordnung der Cache-Funktion von Google abzulehnen, da die Zwischenspeicherung nicht aufgrund einer vorherigen Anfrage eines Nutzers, sondern aufgrund des Einsatzes eines Googlebots von Google selbst vorgenommen wird.[1896]

IV. Access-Provider

Die Haftungsprivilegien des Access-Providers spielen sowohl in Deutschland als auch in den USA keine nennenswerte Rolle. In Deutschland hat dies den Hintergrund, dass der BGH dem Access-Provider ohne Berücksichtigung der spezifischen Bestimmungen

[1893] Siehe hierzu S. 82.
[1894] Siehe hierzu S. 369.
[1895] Siehe hierzu S. 318.
[1896] Im Ergebnis auch eine entsprechende Anwendung ablehnend: Ott in BeckOK InfoMedienR, § 9 TMG, Rn. 28.

des § 8 TMG eine Störerrolle zuspricht und diesem im Rahmen dessen die von ihm entwickelten Prüfpflichten für den Host-Provider aufbürdet. Zudem wird die Privilegierung bislang nicht auf WLAN-Anbieter angewandt.

Auch in den USA haben sich kaum Gerichte mit den genauen Voraussetzungen der *safe habor*-Privilegien des Access-Providers beschäftigt. Dies liegt allerdings vor allem daran, dass aufgrund der weitreichenden Privilegierung ohne Anknüpfung an eine etwaige Kenntnis, eine Inanspruchnahme des Access-Providers nicht aussichtsreich erscheint. Urheberrechteinhaber haben sich daher auf privatrechtliche Vereinbarungen mit den Access-Providern konzentriert oder versuchen ihre Rechte über die Inanspruchnahme der Access-Provider zur Identifizierung ihrer Nutzer durchzusetzen.

1. Sperrpflichten

Die öffentliche Debatte im Hinblick auf den Access-Provider dreht sich in Deutschland größtenteils um seine tatsächliche Möglichkeit und rechtliche Pflicht zur Sperrung von einzelnen Webseiten bzw. URLs. Der BGH hat dem Access-Provider zumutbare Prüfpflichten im Rahmen der Störerhaftung zugesprochen, deren genaue Konturen vollkommen unklar sind.[1897] Zudem hat er die von ihm entwickelten Grundsätze für den Host-Provider auf den Access-Provider übertragen. Die Folge dieser Rechtsprechung ist, dass dem Access-Provider im Rahmen der Störerhaftung nach Kenntnis über eine bestimmte Rechtsverletzung Prüfpflichten im Sinne von Sperrpflichten obliegen, sofern diese für ihn zumutbar sind.[1898] Die Zumutbarkeit setzt zum einen voraus, dass auf der Webseite nach dem Gesamtverhältnis rechtmäßige gegenüber rechtswidrigen Inhalten nicht ins Gewicht fallen sowie zum anderen, dass der Urheberrechtsinhaber zumutbare Anstrengungen unternommen hat, um gegen diejenigen vorzugehen, die die Rechtsverletzung selbst

[1897] Siehe hierzu S. 163.
[1898] Siehe hierzu S. 159.

begangen haben oder die, wie der Host-Provider durch die Erbringung einer Dienstleistung, hierzu beigetragen haben.

Diese Rechtsprechung ist aus mehreren Gründen problematisch. Zunächst bürgt sie dem Access-Provider im Ergebnis eine Pflicht zur Evaluierung des Verhältnisses von rechtmäßigen und rechtswidrigen Inhalten einer von Dritten beanstandeten Webseite auf. Zudem werden ohne Berücksichtigung des § 8 TMG weitere Voraussetzungen geschaffen, die der Access-Provider erfüllen muss, um einer Haftung zu entgehen. Zu guter letzt stehen einer solchen Verpflichtung des Access-Providers auch datenschutzrechtliche Bedenken entgegen.

Im Gegensatz hierzu steht den Urheberrechtsinhabern nach US-amerikanischen Recht im Fall der Anwendbarkeit der *safe harbor* Privilegien lediglich die Möglichkeit zur Erwirkung einer gerichtlichen Anordnung zur Sperrung einer spezifischen Internetseite, welche sich außerhalb der USA befindet, zur Verfügung.[1899] Voraussetzung hierfür ist allerdings, dass zuvor überhaupt erst eine Haftung als direkter oder indirekter Rechtsverletzer festgestellt wird. § 512 (j) DMCA stellt somit keine eigenständige neue Anspruchsgrundlage dar, sondern grenzt die nach den allgemeinen Grundsätzen zur Verfügung stehenden Anordnungen für den Fall, dass der ISP unter den Schutz des *safe harbor* fällt, lediglich ein.

a) Operation In Our Sites

Hinsichtlich Webseiten, welche in den USA registriert sind, hat das US-amerikanische Recht ein anderes Instrument, die Beschlagnahme von Domains (*Domain Name Seizure*), welche unter dem Begriff *Operation In Our Sites* seit 2010 durchgeführt wird.[1900] *Operation In Our Sites* wird koordiniert durch das National Intellectual Property Rights Coordination Center (IPR Center), welches wiederum von ICE verwaltet wird. Das *IPR*

[1899] Siehe hierzu S. 351.

[1900] Siehe allgemein zu *Operation In Our Sites* die Webseite des U.S. Immigration and Customs Enforcement unter https://www.ice.gov/factsheets/ipr-in-our-sites, zuletzt besucht am 24.04.2016.

Center verfügt über 23 *partner agencies*, wie bspw. das FBI und Europol, die bei der Erfüllung seiner Aufgaben eine wesentliche Rolle spielen.[1901] Die Beschlagnahme einer Internetdomain folgt den Bestimmungen des Chapter 46 des Title 18 U.S.C. und läuft wie folgt ab.[1902] Nachdem ICE und das IPR Center mögliche Urheberrechtsverletzungen auf Webseiten ermittelt haben und nach Konsultation mit *DOJ attorneys* (Anwälte des Department of Justice), präsentieren sie einem *federal magistrate judge* eidesstattliche Versicherungen aufgrund dessen dieser bestimmt, ob ein hinreichender Verdacht einer *criminal copyright infringement* vorliegt (sog. *independent probable cause determination*). Sieht er einen hinreichenden Verdacht als gegeben an, erteilt er eine Anordnung zur Beschlagnahme, welche der zuständigen nationalen Domainregistrierungsstelle zugestellt wird. Die Domainregistrierungsstelle ist nach Erhalt der Anordnung verpflichtet, den Domainnamen an eine andere IP-Adresse weiterzuleiten, auf welcher ein Banner erscheint, der den Nutzer darauf hinweist, dass die gegenständliche Domain vom FBI, ICE und IPR-Center beschlagnahmt wurde.

Hauptkritikpunkt an dieser Beschlagnahme ist die fehlende vorherige Benachrichtigung des Webseiten-Betreibers sowie die fehlende vorherige Verteidigungsmöglichkeit zu den ihm vorgeworfenen Verstößen und damit eine Verletzung des 5. Zusatzartikels der Verfassung (*Fifth Amendment*), der das Recht auf ein faires Verfahren (*due process*) garantiert, sowie des 1. Zusatzartikels (*First Amendment*), welcher die Meinungsfreiheit (*free speech*) garantiert.[1903]

Zudem wird kritisiert, dass oftmals gar nicht klar ist, ob der Host-Provider oder der Betreiber einer Link-Seite, dessen Webseite Gegenstand einer Beschlagnahme geworden ist, überhaupt als

---

[1901] Siehe hierzu die Webseite des IPR Center unter https://www.iprcenter.gov/about-us, zuletzt besucht am 24.04.2016.

[1902] Die nachfolgenden Ausführungen zum Ablauf stammen aus Kopel, 28 Berkeley Tech. L.J. 859, 874 ff. (2013).

[1903] Cole, ICE Domain Name Seizures Threaten Due Process and First Amendment Rights; Kopel, 28 Berkeley Tech. L.J. 859, 887 (2013); Minnock, Colo. Tech. L. J. 523, 534 (2014).

direkter Rechtsverletzer angesehen werden kann und dass noch immer nicht geklärt ist, ob eine *secondary liability* überhaupt als Basis für eine strafrechtliche Verantwortlichkeit herangezogen werden kann.[1904]

b) Ergebnis

Auch wenn der Access-Provider unter den *safe harbor*-Privilegien nicht zur Sperrung einer Webseite verpflichtet werden kann, sofern sich diese in den USA befindet, wurde mit *Operation In Our Sites* ein Verfahren entwickelt, welches sowohl Host-Provider als Anbieter von Link-Seiten durch die durch Beschlagnahmung faktische Sperrung ihrer Webseite empfindlich treffen kann, ohne dass diese die vorherige Möglichkeit haben, sich gegen eine Beschlagnahme zur Wehr zu setzen. Damit sind zwar die Access-Provider aus der Schusslinie, dahingegen werden die Bestimmungen des DMCA jedoch dadurch unterlaufen, dass die Host-Provider und Linkseiten-Anbieter erst gar keine Möglichkeit erhalten, durch Einhaltung des *Notice and Takedown*-Verfahrens eine Privilegierung in Anspruch zu nehmen und damit auch ihren Dienst vor einer Beschlagnahme zu schützen. Insoweit sind jedenfalls die Ausführungen des BGH zu begrüßen, dass vor der Sperrung einer Webseite durch den Access-Provider, der Rechteinhaber erfolglos den eigentlichen Rechtsverletzer bzw. den Host-Provider in Anspruch genommen haben muss.[1905]

2. Haftung der WLAN-Betreiber

Die haftungsrechtliche Situation gewerblicher und privater WLAN-Betreiber ist nach deutschem Recht größtenteils unklar. Nach Inkrafttreten das WLAN-Gesetzes ist nun zwar ausdrücklich gesetzlich festgeschrieben, dass § 8 TMG auch für Anbieter drahtloser Netzwerke gilt. Es besteht aber weiterhin Unsicherheit dahingehend, ob § 8 TMG auch für private oder nur für

[1904] Kopel, 28 Berkeley Tech. L.J. 859, 893 (2013). Zu dieser generellen Problematik der strafrechtlichen Verantwortlichkeit eines *indirect infringers* siehe S. 366.
[1905] Siehe hierzu S. 159.

gewerbliche WLAN-Betreiber gilt. Zum anderen hat das WLAN-Gesetz keine Klärung hinsichtlich der Anwendbarkeit des § 8 TMG auf Unterlassungsansprüche sowie im Rahmen der Störerhaftung etwaig bestehender Prüfpflichten sowie deren genauen Konturen gebracht.[1906]

Folge dieser unsicheren rechtlichen Lage ist, dass Privatleute und Gewerbetreibende oftmals vor dem Anbieten eines offenen WLAN Abstand nehmen, was zu einer unterentwickelten Verbreitung offener WLANs im öffentlichen Raum führt.

Im Gegensatz hierzu ist davon auszugehen, dass die Privilegien des DMCA auch auf Anbieter offener WLANs Anwendung finden.[1907] Im Übrigen ist auch ungeachtet der Privilegien eine erfolgreiche Inanspruchnahme aufgrund *secondary copyright infringement* äußerst unwahrscheinlich.[1908] Auch sofern Gerichte eine weite Auslegung des Merkmals der *material contribution* vornehmen würden, ist fraglich, ob dies zu einer Haftung des WLAN-Betreibers führen würde. Nach derzeitigem Kenntnisstand ist dies nicht anzunehmen.[1909]

3. Warnhinweismodell

In Deutschland ist die Diskussion um die Einführung eines Warnhinweismodells aufgrund der diesem Modell zahlreich entgegengebrachten rechtlichen Bedenken zum Erliegen gekommen. Insbesondere die Privatisierung der Rechtsdurchsetzung, der hohe administrative Aufwand und die damit verbunden Kosten sowie die Unvereinbarkeit mit geltendem Datenschutzrecht stehen der Einführung eines solchen Modells entgegen.[1910]

Auch in den USA wurden all diese Bedenken von Kritikern des *Copyright Alert System*, hauptsächlich nach Einführung dieses Systems, vorgebracht.[1911] Zudem wird auch von Seiten der

[1906] Siehe hierzu S. 95.
[1907] Siehe hierzu S. 323.
[1908] Siehe hierzu S. 377.
[1909] Siehe hierzu S. 377.
[1910] Siehe hierzu S. 229.
[1911] Siehe hierzu S. 389. Sehr anschaulich hinsichtlich der Kritikpunkte

Inhalteindustrie vermehrt Kritik gegen das System laut. Im April 2015 haben sich fünf kleine Filmgesellschaften zusammengeschlossen und die *Internet Security Task Force* gegründet mit dem Ziel kleinere Unternehmen der Inhalteindustrie zu mobilisieren um gegen Online-Piraterie zu ankämpfen.[1912] Nach Auffassung der *Internet Security Task Force* ist das *Copyright Alert System* nicht nur ineffektiv, sondern verschlechtere zudem die Lage der Rechteinhaber.[1913] Sie fordern daher eine Einstellung des *Copyright Alert Systems* und die Ablösung durch ein effektiveres System.[1914] Aufgrund der Kritik von allen Seiten kann zu Recht die Frage aufgeworfen werden, ob überhaupt jemand, und wenn ja, wer, von diesem System profitiert.

V. Sonstige ISP

In Deutschland sind Linksetzende und Suchmaschinenanbieter nicht von den Haftungsprivilegien erfasst.[1915] Ihre Verantwortlichkeit richtet sich nach den allgemeinen Grundsätzen. Die Rechtsprechung orientiert sich vornehmlich an der Rechtsprechung des Host-Providers, weshalb auch hier i.d.R. eine Abmahnung durch den Urheber hinsichtlich einer spezifischen Rechtsverletzung vorausgesetzt wird, um die Prüfpflicht des Linksetzenden bzw. Suchmaschinenbetreibers zu begründen. Hinsichtlich des Linksetzenden geht der I. Zivilsenat jedoch davon aus, dass der Hinweis sich nicht auf eine klare Rechtsverletzung beziehen müsse, sondern der Linksetzende nach einem Hinweis auf eine Rechtsverletzung verpflichtet sei, die verlinkte Internetseite zu überprüfen.[1916] Er begründet dies damit, dass sich, im Gegensatz zu dem von der Rechtsordnung gebilligten Host-Provider, Links

---

gegenüber dem Copyright Alert System: Bridy, 23 Fordham Intell. Prop. Media & Ent. L.J. 1 (2012).

[1912] Cieply, Small Film Producers Form a Group to Counter Privacy. Webseite der Internet Security Task Force: http://internetsecuritytaskforce.org.

[1913] Johnson: Producers' Coalition Says Copyright Alert System Has Failed to Stop Piracy.

[1914] Johnson: Producers' Coalition Says Copyright Alert System Has Failed to Stop Piracy.

[1915] Siehe hierzu S. 112.

[1916] Siehe hierzu S. 187.

oftmals auf kommerziellen Webseiten befänden, die lediglich ein zusätzliches Informationsangebot hinzufügten und es sich zumeist um eine begrenzte Anzahl von Hyperlinks handele. Die genauen Konturen dieser vom BGH vorgenommenen Abgrenzung sind jedoch unklar. Das Resultat dürfte im Zweifel eine Verpflichtung zur inhaltlichen Überprüfung jedweder Anzeige auf eine Rechtsverletzung darstellen. Aufgrund der expliziten Bezugnahme auf die begrenzte Anzahl von Hyperlinks kann allerdings als gesichert gelten, dass der Suchmaschinenanbieter von dieser Verpflichtung befreit ist.

Zudem birgt insbesondere die neueste Rechtsprechung im Hinblick auf das Framing von fremden Inhalten welche ohne Erlaubnis des Rechteinhabers ins Internet gestellt wurden, die Gefahr, eine ausufernde Haftung des Linksetzenden sowie Suchmaschinenanbieters zu begründen.[1917] Im Rahmen dieser Rechtsprechung ist derjenige, der Inhalte auf seiner Webseite einbettet als Täter für die öffentliche Zugänglichmachung verantwortlich, sofern der eingebettete Inhalt ursprünglich rechtswidrig ins Internet eingestellte wurde. Er sehe sich somit auch Schadensersatzansprüchen ausgesetzt. Eine Übertragung dieser Grundsätze wäre ohne Weiteres auch auf den einfachen Linksetzenden sowie Suchmaschinenbetreiber denkbar.

In den USA ist der Linksetzende und Suchmaschinenbetreiber hingegen von dem *safe harbor* des DMCA für *Information Location Tools* erfasst. Die Privilegierung unterliegt ähnlichen Voraussetzungen wie die des Host-Providers.[1918] Er fällt folglich unter den *safe harbor*, sofern er keine *actual* oder *red flag knowledge* hat oder nach Erhalt einer *notification* den Link zu dem beanstandeten Material entfernt bzw. sperrt. Der Vorteil an diesem gesetzlich festgeschriebenem *safe harbor* liegt an den genauen Vorgaben zur Entgehung einer Verantwortlichkeit und einer damit einhergehenden Rechtssicherheit für *Information Location Tools*.

[1917] Siehe hierzu S. 199.
[1918] Siehe hierzu S. 325.

Im Unterschied zum Host-Provider gibt es bei einem *takedown* durch *Information Location Tools* jedoch keine Möglichkeit der Verteidigung und Wiederherstellung der Verlinkung. Auch wenn sich der Inhalt nach Entfernung des Links noch an seinem Ursprungsort befindet, sorgen die *Information Location Tools* in der Praxis maßgeblich für die Auffindbarkeit von Inhalten.

VI. Ergebnis

Das US-amerikanische System bietet dem ISP insbesondere mit klaren Bestimmungen zum *takedown* und einer diesbezüglich gesetzlich geregelten Haftungsprivilegierung, welche *injunctions* nur in einem äußerst engen Rahmen zulässt, einen erheblich höheren Grad an Rechtssicherheit als das durch die Rechtsprechung in Deutschland entwickelte System der Störerhaftung. Die Rechtsprechung der US-amerikanischen Gerichte zieht die Bestimmungen des DMCA unter Bezugnahme auf den Sinn und Zweck des safe *harbor* maßgeblich in seine Bewertung der Verantwortlichkeit der ISP mit ein.

F. Schlussbetrachtung und Lösungsansätze

I. Verifizierung der Arbeitshypothese

Diese Arbeit ging von der Annahme aus, dass durch die Ausweitung der Privilegien durch die Rechtsprechung, die gesetzlich auf europäischen Vorgaben basierenden Haftungsprivilegien der ISP faktisch entwertet werden und entsprechend die Ziele der Privilegien nicht erreicht wurden und eine gerechte Balance der Interessen der Akteure nicht hergestellt wurde.

Wie innerhalb der Untersuchung der deutschen Rechtsprechung zur Haftung der ISP für Rechtsverletzungen Dritter aufgezeigt wurde, haben die deutschen Gerichte ein System entwickelt, welches die Bestimmungen des TMG weitgehend außer Acht lässt und sich maßgeblich auf die Grundsätze der deutschen Störerhaftung stützt. Legitimiert wird dies durch § 7 Abs. 2 S. 2 TMG, welcher

Verpflichtungen zur Entfernung oder Sperrung nach den allgemeinen Grundsätzen unberührt lässt. Es ist davon auszugehen, dass der deutsche Gesetzgeber die europarechtlichen Vorgaben hiermit nicht adäquat umgesetzt hat. Denn im Gegensatz zur deutschen Störerhaftung, auf die sich unmittelbar aufgrund der Unberührtheit der allgemeinen Grundsätze gestützt wird, sehen die europäischen Vorgaben sowohl innerhalb der ECRL als auch die InfoSoc-RL lediglich die Möglichkeit gerichtlicher Anordnungen vor. Im Gegensatz hierzu wird dem ISP im Rahmen der Störerhaftung eine Prüfpflicht auferlegt, welche i.d.R. an die Kenntnis des ISP über eine Rechtsverletzung anknüpft und ihm eine der Unterlassungspflicht in ihrem Ergebnis gleichkommende Verpflichtung auferlegt, jedoch ohne gerichtliche Beteiligung.

Maßgeblich zur Unsicherheit der ISP trägt der nicht klar umrissene Umfang einer solchen dem ISP auferlegten Prüfpflicht bei. Durch die Ausweitung auf kerngleiche Rechtsverstöße wird der ISP faktisch dazu verpflichtet, sämtlichen Datenverkehr zu filtern und zu überprüfen. Diese Rechtsprechungsentwicklung steht im Widerspruch zu den Zielen des deutschen sowie europäischen Gesetzgebers. Der ISP sieht sich in Deutschland noch immer Gefahren für sein Geschäftsmodell ausgesetzt. So können die Prüfpflichten und eine damit zusammenhängende etwaige Unterlassungsverpflichtung den ISP in seinem Geschäftsmodell empfindlich treffen. Anschauliches Resultat einer solch potentiellen Gefahr ist die Unterentwicklung von offenem WLAN in Deutschland. Die Schaffung von Rechtssicherheit zur Förderung innovativer Geschäftsmodelle ist folglich nicht erreicht worden.

Wie die Analyse des US-amerikanischen Rechts gezeigt hat, ist das materielle Recht im Kern dem des deutschen Rechts sehr ähnlich. Entscheidender Unterschied ist jedoch das *Notice and Takedown*-Verfahren des US-amerikanischen Rechts, welches durch gesetzlich genau definierte Vorgaben dem Cache- und Host-Provider sowie den *Information Location Tools* das erforderliche Maß an Rechtssicherheit verschafft. Im Gegensatz zur deutschen

Rechtsprechung wenden die US-amerikanischen Gerichte die Haftungsprivilegien zudem konsequent bei der Beurteilung der Verantwortlichkeit der ISP an. Insbesondere der Access-Provider genießt eine, seiner rein technisch und neutralen Funktion adäquate, weitreichende Haftungsprivilegierung, welche nicht durch die Begründung irgendwie gearteter Prüfpflichten untergraben wird.

Entsprechend genießen ISP in den USA eine angemessene Rechtssicherheit, welche sie in der Errichtung und dem Betrieb ihrer Geschäftsmodelle in gebührender Weise fördert.

Die Arbeitshypothese konnte folglich vollständig verifiziert werden.

II. Lösungsmodell

Um die verschiedenen Geschäftsmodelle der ISP auf ein rechtssicheres Fundament zu stellen, ist eine Reihe von Lösungsansätzen denkbar.

1. Anwendbarkeit auf Unterlassungsansprüche

Substantiell für die Schaffung von Rechtssicherheit ist die konsequente Anwendung der §§ 8-10 TMG auf Unterlassungsansprüche. Es sollte daher klargestellt werden, dass auch Unterlassungsansprüche grundsätzlich von den Haftungsprivilegien des TMG umfasst sind. Dies entspricht den europäischen Vorgaben und dient dem Ziel die ISP vor ausufernden Prüfpflichten ohne gerichtliche Intervention zu schützen. Möglich bleiben sollten aber weiterhin gerichtliche Anordnungen zur Entfernung oder Sperrung von bestimmten Inhalten. Diese dürfen aber nicht mehr, wie bisher, von der Verletzung irgendwie gearteter Prüfpflichten im Rahmen der Störerhaftung abhängig gemacht werden, sondern haben sich an den Vorgaben der §§ 8-10 TMG zu orientieren.

a) Host-Provider

Im Falle des Host-Providers bedeutet dies in richtlinienkonformer Auslegung das Folgende. Der Host-Provider ist zunächst

entsprechend § 10 TMG ohne Kenntnis einer Urheberrechtsverletzung nicht verantwortlich. Erlangt er Kenntnis einer Rechtsverletzung i.S.d. § 10 TMG, so hat er den rechtsverletzenden Inhalt zu entfernen bzw. zu sperren. Versäumt er dies, hat der Urheberrechtsinhaber gegen den Host-Provider einen durchsetzbaren Anspruch auf Beseitigung und Unterlassung. Dieser sollte jedoch beschränkt sein auf die Entfernung des spezifisch beanstandeten Inhaltes und nicht ausgedehnt werden auf zukünftige kerngleiche Rechtsverletzungen.[1919] Denn ein Anspruch auf zukünftige Unterlassung gleichartiger Rechtsverstöße bezieht sich weder auf einen bestimmten Nutzer noch auf eine bestimmte Zeit und stellt daher eine generelle Überwachungsverpflichtung des Host-Providers i.S.d. § 7 Abs. 2 S. 1 TMG dar und keine in einem spezifischen Fall. [1920] Eine Anwendung der Kerntheorie ist deshalb abzulehnen.

Als Grundlage für die Beseitigungs- und Unterlassungsverpflichtung des Host-Providers dient wie bisher die Störerhaftung, die Pflichtverletzung liegt aber in dem Versäumnis der Sperrung bzw. Entfernung des rechtsverletzenden Inhaltes nach Kenntnis.

Dies steht auch im Einklang mit der vom BGH bislang vertretenen Ansicht, dass die Erstabmahnung bzw. der erste Hinweis auf eine Rechtsverletzung grundsätzlich keine Haftung des Host-Providers begründet. Denn der Hinweis auf die Rechtsverletzung an sich wirkt insoweit, dass er lediglich eine Pflicht zur Entfernung bzw. Sperrung des rechtsverletzenden Inhaltes auslöst. Diese Pflicht trifft den Host-Provider als Prüfpflicht, um einer Inanspruchnahme als Störer zu entgehen. Kommt er dieser Prüfpflicht nicht nach, haftet er als Störer und dem Urheberrechtsinhaber steht entsprechend ein Anspruch auf Beseitigung und Unterlassung gegen den Host-Provider als Störer zu.

[1919] Hierfür im Ergebnis auch Sieber/Höfinger in Hoeren/Sieber/Holznagel, Teil 18.1, Rn. 60; Hoeren in Festschrift für Ulrich Eisenhardt, S. 243, 252.

[1920] So auch Sieber/Höfinger in Hoeren/Sieber/Holznagel, Teil 18.1, Rn. 60; Hoeren in Festschrift für Ulrich Eisenhardt, S. 243, 251.

Prüfpflichten, um der Inanspruchnahme als Störer nach Kenntnis und Entfernung bzw. Sperrung des Inhaltes zu entgehen, gibt es nicht mehr. Entfernt bzw. sperrt der Host-Provider den urheberrechtsverletzenden Inhalt, ist er nach den Vorgaben des § 10 TMG von einer Haftung befreit.

Es bedarf daher im Grunde keiner diesbezüglich expliziten gesetzlichen Regelung. Eine richtlinienkonforme Fortentwicklung des § 10 TMG in Abkehr von seiner bisherigen Leitlinie zur Störerhaftung läge in der Verantwortung des BGH.

Es ist zudem die Aufgabe des BGH, die Prüfpflichten, wie bisher, auf das dem Host-Provider Zumutbare zu beschränken. Hier sollte das Merkmal der Zumutbarkeit so ausgelegt werden, dass ein Verstoß gegen die Prüfpflichten nur in den Fällen vorliegt, in denen er tatsächliche Kenntnis von der Rechtsverletzung hat oder die Rechtsverletzung offensichtlich war. Diese Einschränkung ist im Einklang mit den Voraussetzungen einer Privilegierung des Host-Providers nach § 10 TMG.

Hinsichtlich der konkreten Anforderungen, die notwendig für eine solche Kenntnis bzw. Offensichtlichkeit sind, kann auf den vom BGH in seinem „Stiftparfum“-Urteil etablierten Maßstab zurückgegriffen werden. Danach muss der Host-Provider den Rechtsverstoß unschwer, d.h. ohne eingehende rechtliche und tatsächliche Überprüfung, feststellen können.[1921] Das genaue Ausmaß einer insoweit vom Host-Provider zu verlangenden Prüfung sollte abhängig von den Umständen des Einzelfalls, insbesondere dem Gewicht der behaupteten Rechtsverletzung sowie der Erkenntnismöglichkeit des Host-Providers sein.[1922] Hinsichtlich einer Offensichtlichkeit wird auf die Ausführungen des EuGH zurückgegriffen. Danach ist eine Rechtsverletzung offensichtlich, wenn der Host-Provider sich etwaiger Tatsachen oder Umstände bewusst war, auf Grund derer ein sorgfältiger

[1921] BGH GRUR 2011, 1038, 1040.
[1922] BGH GRUR 2011, 1038, 1040 f.

Wirtschaftsteilnehmer die Rechtswidrigkeit hätte feststellen müssen.[1923]

Durch diese Einschränkung werden die Anforderungen an eine Kenntnis im Sinne des § 10 TMG konsequent angewandt und der Host-Provider bei Fehlen einer entsprechenden Kenntnis wiederum der Privilegierung des § 10 TMG unterstellt. Hierdurch wird den Interessen des Host-Providers und den europäischen Vorgaben ausreichend Rechnung getragen und die Host-Provider werden vor einer ausufernden zivilrechtlichen Verantwortlichkeit geschützt, die das von ihnen betätigte Geschäftsmodell gefährden könnte.

b) Cache-Provider

Entsprechend dem Host-Provider sollte auch die Privilegierung und etwaige Unterlassungsverpflichtung des Cache-Providers ausgestaltet sein. Der Cache-Provider ist privilegiert sofern er gem. § 9 S. 1 Nr. 5 TMG unverzüglich handelt, um gespeicherte Informationen zu entfernen oder den Zugang zu diesen zu sperren, sobald er Kenntnis davon erhalten hat, dass die Information am ursprünglichen Ausgangsort der Übertragung aus dem Netz entfernt wurde bzw. der Zugang zu ihr gesperrt wurde oder ein Gericht oder eine Verwaltungsbehörde die Entfernung bzw. Sperrung angeordnet hat. Sofern der Cache-Provider entgegen § 9 TMG urheberrechtsverletzende Inhalte nach Kenntnis über die Entfernung bzw. Sperrung des rechtsverletzenden Inhalts am Ursprungsort bzw. einer entsprechenden Anordnung zur Entfernung bzw. Sperrung nicht entfernt oder sperrt, bemisst sich seine Verantwortlichkeit nach den allgemeinen Gesetzen. Allerdings wird im Falle des Cache-Providers eine Haftung als Störer aufgrund der Verletzung zumutbarer Prüfpflichten regelmäßig gegeben sein, sofern er die beanstandeten Informationen nicht entfernt oder sperrt, obwohl diese am Ursprungsort entfernt wurden. Denn im Unterschied zum Host-Provider knüpft die Sperrung bzw. Entfernung des Cache-Providers nicht an die Kenntnis der Rechtswidrigkeit des Inhalts an, sondern

[1923] EuGH, MMR 2011, 596, 603.

lediglich daran, dass Kenntnis darüber besteht, dass der beanstandete Inhalt am Ausgangsort der Übertragung entfernt oder gesperrt wurde bzw. eine entsprechende gerichtliche Anordnung hinsichtlich einer solchen Entfernung bzw. Sperrung vorliegt.

c) Linksetzende

Auch der Linksetzende ist grundsätzlich hinsichtlich etwaiger Unterlassungsansprüche privilegiert, sofern er Links zu urheberrechtsverletzenden Inhalten nach Kenntnis entfernt bzw. sperrt. Der Unterlassungsanspruch gegen den Linksetzenden sollte sich dementsprechend an einer nicht erfolgten Entfernung bzw. Sperrung von Links zu urheberrechtsverletzenden Inhalten orientieren. Hat der Linksetzende Kenntnis über rechtsverletzende Inhalte, auf die er verlinkt und entfernt er daraufhin nicht die Links zu den rechtsverletzenden Inhalten, so ist er hierfür nach den allgemeinen Gesetzen verantwortlich. Dies bedeutet, dass der Rechteinhaber, sofern der Linksetzende zumutbare Prüfpflichten verletzt hat, einen Unterlassungsanspruch gegen den Linksetzenden geltend machen kann. Hinsichtlich der Zumutbarkeit ist, wie auch beim Host-Provider, auf die Erkennbarkeit der Rechtsverletzung abzustellen.

d) Access-Provider

Im Unterschied zu den anderen ISP sollte im Hinblick auf den Access-Provider eine explizite gesetzliche Regelung hinsichtlich möglicher gerichtlicher Anordnungen erlassen werden. Dies beruht auf der folgenden Überlegung. Anders als bei dem Host- und Cache-Provider sowie dem Linksetzenden, ist die Privilegierung des Access-Providers grundsätzlich unabhängig von einer etwaigen Kenntnis über eine bestimmte Rechtsverletzung. Da der Access-Provider im Rahmen seiner Tätigkeit i.d.R. keine Kontrolle über die Inhalte hat, zu denen er Zugang vermittelt und sich seine Tätigkeit insoweit auf die Zurverfügungstellung der technischen Infrastruktur beschränkt, erscheint das Konstrukt der Störerhaftung mit der Auferlegung von Prüfpflichten im Fall des Access-

Providers nicht gerechtfertigt.[1924] Dies spiegelt sich entsprechend auch in der weiten, von einer Kenntnis unabhängigen Privilegierung, wider. Im sichtlichem Widerspruch zu der umfassenden Privilegierung des Access-Providers steht jedoch die sehr weite Kausalitätsbetrachtung des allgemeinen Deliktsrechts.[1925] Da jedoch auch gegen den Access-Provider nach Art. 8 Abs. 3 InfoSoc-RL sowie nach der Rechtsprechung des EuGH gerichtliche Anordnungen zum Schutz der Urheberrechte ermöglicht werden müssen, bedarf es hier einer expliziten Regelung. Denn einer solchen Anordnung gegen den Access-Provider liegt keine Verantwortlichkeit im Sinne des Deliktrechts zugrunde, sondern vielmehr der Gedanke, dass dieser am besten in der Lage ist, den Rechtsverstößen ein Ende zu setzen.[1926]

Es wird daher auf einen bereits im Schrifttum von *Hofmann* formulierten Vorschlag einer Vorschrift analog des Auskunftsanspruches gem. §§ 101 Abs. 2 S. 1 Nr. 2, 101 Abs. 9 UrhG zurückgegriffen.[1927]

Analog des Auskunftsanspruches gegen Vermittler sollte auch die Anordnung zur Sperrung rechtsverletzender Internetseiten gegen den Access-Provider unabhängig von einer etwaigen Verantwortlichkeit des Access-Providers erfolgen.[1928] Zudem würde eine richterliche Anordnung den Interessen der Internetnutzer Rechnung tragen sowie die Entscheidung und damit einhergehende Bewertung der als rechtsverletzend geltend gemachten Webseite und der Grundrechtsabwägung im Einzelfall nicht dem Access-Provider auferlegen.[1929] Auch würde dem durch die Sperrung seiner

[1924] So im Ergebnis auch Czychowski/Nordemann, GRUR 2013, 986, 990, die allerdings bereits den erforderlichen willentlich und adäquat kausalen Verletzungsbeitrag als nicht gegeben ansehen und insoweit die Störerhaftung richtlinienkonform im Bereich des Immaterialgüterrechts auslegen wollen; zweifelnd hinsichtlich des Verursachungsbeitrages des Access-Providers auch Leistner/Grisse, GRUR 2015, 19, 20.
[1925] Zutreffend auf die sehr weite Kausalität hinweisend auch Peifer, AfP 1/2014, 18, 21.
[1926] Siehe hierzu Erwägungsgrund 59 der InfoSoc-RL; Czychowski/Nordemann, GRUR 2013, 986, 989.
[1927] Hofmann, NJW 2016, 796, 771; Hofmann, GRUR 2015, 123, 129 f.
[1928] Hofmann, GRUR 2015, 123, 129.
[1929] Hofmann, GRUR 2015, 123, 129.

Internetseite betroffenen Inhalteanbieter die Möglichkeit offen stehen, eine Beschwerde gegen die gerichtliche Anordnung gem. §§ 58, 59 FamFG zu erwirken, was zu einer Stärkung der Rechte des Inhalteanbieters führen würde.[1930]

Diesbezüglich sollte der Access-Provider allerdings nur subsidiär in Anspruch genommen werden können. Dies entspricht auch den Ausführungen des BGH in seinem „Goldesel"-Urteil[1931]. Wenngleich der BGH diesen Grundsatz der Subsidiarität des Access-Providers über Bande bereits begründet hat, sollte die Subsidiarität gesetzlich verankert werden.

Durch diese Möglichkeit der gerichtlichen Anordnung würde die bisherige Störerhaftung mit der Auferlegung von Prüfpflichten des Access-Providers zudem vollständig verdrängt.

e) Änderung des TMG

Entsprechend sollte § 7 Abs. 2 S. 2 TMG vom Wortlaut dahingehend abgeändert werden, dass der Bezug auf die *Verpflichtungen zur Entfernung und Sperrung der Nutzung von Informationen nach den allgemeinen Gesetzen* entfernt wird. Dass in Fällen, in denen die Tätigkeit des ISP aus den Privilegien des TMG herausfällt, die allgemeinen Gesetze Anwendung finden, bedarf keiner expliziten Benennung.

2. Zu eigen Machen/aktiver ISP

Die Gerichte sollten zudem ein zu eigen Machen fremder Inhalte nur in engen Grenzen zulassen. Für ein zu eigen Machen ausreichend darf jedenfalls nicht die Tatsache sein, dass der Provider Überprüfungsmaßnahmen aus eigener Motivation durchführt und in diesem Zusammenhang bestimmte Materialien sichtet. Würde man in diesem Fall bereits von einem zu eigen Machen von fremden Inhalten ausgehen, so würden damit sämtliche Bemühungen der ISP bestimmte rechtswidrige Tätigkeiten aufzudecken konterkariert. Es würden hierdurch vielmehr Anreize geschaffen, bestimmte Kontrollmaßnahmen nicht

[1930] Hofmann, GRUR 2015, 123, 129.
[1931] Siehe hierzu S. 159.

durchzuführen, da der ISP hierdurch Gefahr laufen würde, als Täter die volle Verantwortung für die Inhalte seiner Nutzer zu tragen. Ein zu eigen Machen sollte entsprechend von den Gerichten nur in den Fällen angenommen werden, in denen der ISP nach außen hin erkennbar den Inhalt als seinen eigenen Inhalt in voller Kenntnis der Rechtswidrigkeit in seinen Dienst integriert oder diesen durch eindeutige Bezugnahme auf dessen Rechtswidrigkeit bewirbt. Dies dürfte auch dem Willen der Bundesregierung entsprechen, welche eben diesen Fall der Förderung von Rechtsverletzungen durch eigene Maßnahmen mit dem momentan nicht weiter verfolgten Gesetzesentwurf zur Änderung des TMG und einer vermuteten Kenntnis des Host-Providers abdecken wollte.[1932] Im Gegensatz hierzu würde der diesseitige Vorschlag aber im Einklang mit europäischen Vorgaben stehen.

Der EuGH hat bereits in seiner „L'Oréal"-Rechtsprechung ausgeführt, dass die Privilegien der ECRL lediglich auf neutrale ISP Anwendung finden.[1933] Auch wenn diese Rechtsprechung des EuGH insbesondere aufgrund ihrer Herleitung durchaus kritikwürdig ist, so eignet sich der Grundgedanke der Abgrenzung eines neutralen und aktiven ISP durchaus, um solche ISP, deren Dienst offensichtlich auf Rechtsverletzungen ausgelegt ist und die eine rechtswidrige Verwendung durch eigene Maßnahmen fördern, von den Privilegien des TMG auszuschließen. Der EuGH stellt hinsichtlich des aktiven ISP darauf ab, dass diesem durch bestimmte Handlungen eine aktive Rolle zukommt, die ihm eine Kenntnis oder eine Kontrolle der streitgegenständlichen Inhalte verschafft. Während die Kenntnis eines spezifischen Inhaltes auch im Fall eines aktiven Providers i.d.R. schwierig nachzuweisen sein wird, könnte dennoch eine Kontrolle dieser Inhalte bejaht werden. Der Gerichtshof hat nicht weiter ausgeführt, was genau unter einer

[1932] Siehe hierzu S. 55.

[1933] Siehe hierzu S. 46. Aus diesem Grund bedarf es auch keiner Reform der ECRL, die *Ohly* anspricht, um den überholten bipolaren Ansatz, welcher lediglich zwischen fremden und eigenen Informationen unterscheidet, einer differenzierteren Lösung, insbesonder im Hinblick auf Tätigkeiten im Grenzbereich zwischen rein passiver Tätigkeit und aktiver Hilfestellung, zuzuführen, siehe Ohly, ZUM 2015, 308, 313.

solchen Kontrolle zu verstehen ist. Es wird dem nationalen Recht insoweit ein gewisser Spielraum zuteil. Rückschlüsse können diesbezüglich aus dem US-amerikanischen Recht und der *right and ability to control* gezogen werden. Insoweit könnte bspw. eine Kontrolle bejaht werden, sofern der ISP durch zielgerichtetes Verhalten Rechtsverletzungen fördert oder erheblichen Einfluss auf die Nutzer und deren rechtswidrige Handlungen ausübt. Ist dies hinsichtlich des Dienstes des ISP der Fall, so kann dem ISP auch im Hinblick auf den spezifischen streitgegenständlichen Inhalt eine entsprechende Kontrolle zugerechnet werden. Die Gerichte hätten hierdurch die Möglichkeit, im Einzelfall einem solch aktiven ISP die Haftungsprivilegierung zu versagen.

Einer gesetzlichen Änderung bedarf es diesbezüglich jedoch nicht. Den Gerichten bleibt es unbenommen, im Rahmen einer Einzelfallabwägung aktiven Providern, die durch ihre Handlungen Rechtsverletzungen vorsätzlich fördern, eine Privilegierung zu versagen. Sofern dies in einem eng abgesteckten Rahmen geschieht, steht dies auch nicht dem Ziel der Schaffung von Rechtssicherheit entgegen. Betroffen wären insoweit nur solche ISP, die ein Geschäftsmodell mit dem Ziel betreiben, aus der Verletzung von Urheberrechten Profit zu schlagen. Die Gerichte wären hier jedoch angehalten, diesbezüglich klare Leitlinien zu entwickeln, um eine ausufernde Rechtsprechung zu unterbinden.

3. Sonstige Providerspezifische Regelungen

Zusätzlich wären zur Stärkung der Position der einzelnen ISP die folgenden Änderungen erwägenswert, welche nach diesseitiger Auffassung jedoch nicht zwingend notwendig sind.

a) Host-Provider

Obgleich die Einbeziehung von Unterlassungsansprüchen als wichtigstes Instrument zur Schaffung von Rechtssicherheit des Host-Providers und damit der Förderung der Ziele des deutschen und europäischen Gesetzgebers dient, sind noch weitere Änderungen der bestehenden Regelung zur Haftungsprivilegierung

des Host-Providers der Schaffung von Rechtssicherheit zweckdienlich.

aa) Notice and Takedown-Verfahren

In der Praxis erfolgt auch nach dem derzeitigen Modell der Großteil der Löschungen bzw. Sperrungen aufgrund von Hinweisen von Rechteinhabern. Obwohl § 10 TMG auf die Kenntnis bzw. das Kennenmüssen abstellt, sind Host-Provider aufgrund der unsicheren Rechtslage dazu motiviert, Inhalte aufgrund eines Hinweises ungeprüft zu löschen. Kritisch hieran ist insbesondere, dass aufgrund fehlender gesetzlicher Bestimmungen dahingehend, welche Angaben ein solcher Hinweis zu enthalten hat, ein erhebliches Missbrauchspotential besteht. Um dieses einzudämmen und um dem Host-Provider klare Leitlinien an die Hand zu geben, könnten die Voraussetzungen, die an einen solchen Hinweis zu stellen sind, gesetzlich festgeschrieben werden.[1934] Diese gesetzliche Festschreibung kann in Anlehnung an die US-amerikanischen *notifications* erfolgen, sollte aber die an der US-amerikanischen Regelung geäußerten Kritikpunkte angemessen berücksichtigen.

Insbesondere sollte den Interessen der Inhalteanbieter angemessen dadurch Rechnung getragen werden, dass eine kurze materiell-rechtliche Begründung des Anspruchs dem Hinweis beizufügen ist.[1935]

Der Host-Provider sollte nach Erhalt des formell korrekten Hinweises zu keiner Prüfung der darin enthaltenen Angaben verpflichtet sein. Zum Erhalt seiner Privilegierung sollte er lediglich das Material unverzüglich zu entfernen oder zu sperren haben. Zusätzlich sollte er jedoch analog der US-amerikanischen Regelung dazu verpflichtet werden, eine Kopie des Hinweises an den vermeintlichen Rechtsverletzer weiterzuleiten. Hierdurch wird sichergestellt, dass der behauptete Rechtsverletzer Kenntnis über den geltend gemachten Anspruch des Rechteinhabers erhält.

[1934] Eine entsprechende *Notice and Takedown*-Regelung vorschlagend auch Holznagel, S. 246 ff.
[1935] So auch Holznagel, S. 251.

Zudem sollte dem Nutzer, dessen Inhalte Gegenstand eines solchen Hinweises sind, die Möglichkeit eröffnet werden, sich gegen die Behauptung der Urheberrechtsverletzung zu verteidigen. Auch hier kann als Grundlage für die inhaltliche Ausgestaltung einer solchen Gegendarstellung auf die Regelung des DMCA zurückgegriffen werden. Allerdings sollte zusätzlich innerhalb der Gegendarstellung hinsichtlich der Unbegründetheit des geltend gemachten Anspruches ausgeführt werden.[1936]

Nach Erhalt der Gegendarstellung des vermeintlichen Rechtsverletzers sollte der Host-Provider dazu verpflichtet sein, das Material unverzüglich wieder zugänglich zu machen. Im Gegensatz zum US-amerikanischen Modell wird hier zu Gunsten des behaupteten Rechtsverletzers auf eine Übergangsfrist verzichtet.[1937] Dies scheint insbesondere vor dem Hintergrund, dass auch die Löschung des beanstandeten Inhaltes unverzüglich nach Erhalt des Hinweises erfolgt, interessengerecht. Zugleich hat der Host-Provider eine Kopie der Gegenanzeige an den ursprünglichen Versender des Hinweises weiterzuleiten, allerdings ohne die die Person des vermeintlichen Rechtsverletzers identifizierenden Angaben.

Dem Rechteinhaber bleibt es in der Folge noch immer unbenommen, einen Auskunftsanspruch gegen den Host-Provider geltend zu machen und schließlich ein gerichtliches Verfahren gegen den vermeintlichen Rechtsverletzer einzuleiten.

Klarstellend wird auch eine Regelung eingefügt, dass ein Hinweis bzw. eine Gegendarstellung, welche nicht den Anforderungen der gesetzlichen Bestimmung entspricht, unbeachtet bleiben kann.

bb) Haftungsfreistellung ggü. Nutzer und Rechteinhaber

Sofern der Host-Provider das gesetzlich festgelegte *Notice and Takedown*-Verfahren einhält, sollte er sowohl gegenüber dem

[1936] So auch Holznagel, S. 251.

[1937] Anders Holznagel, 252, der die Wiedereinstellung erst nach 7 Werktagen vornehmen will und lediglich dann, wenn innerhalb dieser Zeit keine Mitteilung des Urheberrechtsinhabers eingeht, dass dieser gerichtliche Schritte gegen den Nutzer eingeleitet hat oder solche nicht möglich sind.

Nutzer für den *takedown* als auch gegenüber dem Rechteinhaber hinsichtlich einer späteren Wiederherstellung des Inhaltes aufgrund einer Gegendarstellung freigestellt werden. Diese Haftungsfreistellung trägt maßgeblich zur Rechtssicherheit des Host-Providers bei und stellt sicher, dass dieser keine Ansprüche des Nutzers oder Rechteinhabers zu befürchten hat.

cc) Haftung für falsche Angaben

Aufgrund der grundsätzlichen Missbrauchsanfälligkeit des *Notice and Takedown*-Systems sollte das TMG ausdrücklich Schadensersatzansprüche des Inhalteanbieters sowie des Urheberrechtsinhabers für grob fahrlässig oder vorsätzlich gemachte falsche Angaben innerhalb des Hinweises und der Gegendarstellung vorsehen. Auch wenn grundsätzlich die Geltendmachung von Ansprüchen nach den allgemeinen Gesetzen möglich ist, so sorgt eine spezifische Regelung innerhalb des Haftungsregimes zum einen für die nötige Rechtssicherheit und dient zum anderen zugleich als Abschreckung.

b) Cache-Provider

Die Bestimmungen hinsichtlich der Privilegierung des Cache-Providers sind grundsätzlich ausreichend, um diesem das erforderliche Maß an Rechtssicherheit zur Betreibung seines Geschäftsmodells zu gewähren. Insbesondere zu begrüßen ist die Kopplung der Verpflichtung zur Entfernung bzw. Sperrung des beanstandeten Inhaltes an die Entfernung bzw. Sperrung auf der Ursprungsseite. Eines den gesetzlichen Vorgaben entsprechenden Hinweises bedarf es jedoch nicht, da durch die Voraussetzung, dass der Inhalt an seinem Ursprungsort entfernt wurde bzw. eine entsprechende gerichtliche Anordnung vorliegt, die Interessen des Inhalteanbieters ausreichend gewahrt sind. In dieser Hinsicht könnte aber ein Zusatz in § 9 TMG aufgenommen werden, dass der Inhalt auch aufgrund eines entsprechenden Hinweises darüber, dass die Information am ursprünglichen Ausgangsort aus dem Netz entfernt wurde oder eine entsprechende Anordnung vorliegt, zu

entfernen oder zu sperren ist. Der Versender des Hinweises hat allerdings unter Angabe seiner Identität zu versichern, dass das streitgegenständliche Material auf der Ursprungsseite entfernt wurde bzw. er eine Kopie der gerichtlichen Anordnung beizufügen hat.

Hierdurch wird auch für den Cache-Provider eine „light"-Version des *Notice and Takedown*-Systems etabliert, welche mit Blick auf den von ihm zur Verfügung gestellten Dienst interessengerecht erscheint.

c) Access-Provider

Die weite Haftungsprivilegierung des § 8 TMG des Access-Providers ist grundsätzlich dazu geeignet, diesem Rechtssicherheit zu gewähren. Die Problematik liegt derzeit vielmehr in der Begründung von Prüfpflichten im Rahmen der Störerhaftung nach entsprechendem Hinweis über eine Rechtsverletzung. Um die sozial erwünschte, üblicherweise auf die Bereitstellung der Infrastruktur begrenzte, Tätigkeit des Access-Providers ausreichend abzusichern, ist eine konsequente Anwendung der Privilegierung durch die Gerichte erforderlich. Im Gegensatz zur Rechtsprechung des BGH sollen den Access-Provider daher keine Prüfpflichten nach Hinweis auf eine Rechtsverletzung treffen.

Um dennoch Art. 12 Abs. 3 ECRL und Art. 8 Abs. 3 InfoSoc-RL Rechnung zu tragen, ist die Möglichkeit einer gerichtlichen Anordnung gegen den Access-Provider vorzusehen. Diese Anordnung kann dann darin bestehen, dass der Access-Provider es unterlässt, den Zugang zu einer spezifischen Internetseite herzustellen, sofern eine solche Anordnung die betroffenen Grundrechte angemessen miteinander abwägt sowie den Schutz personenbezogener Daten sowie das Fernmeldegeheimnis angemessen berücksichtigt.

In § 8 TMG ist entsprechende Regelung hinsichtlich der Möglichkeit einer gerichtlichen Anordnung gegen den Access-Provider zu integrieren. Die inhaltliche Ausgestaltung kann sich an

der Regelung des Auskunftsanspruches gegenüber dem Nichtverletzer des UrhG orientieren.

d) Linksetzende und Suchmaschinenanbieter

Die Verantwortlichkeit des Linksetzenden und des Suchmaschinenanbieters richtet sich derzeit nach den allgemeinen Gesetzen. Von den Privilegien des TMG sind sie nicht erfasst. Auf die Möglichkeit einer Einbeziehung auf europäischer Ebene weist jedoch Artikel 21 Abs. 2 ECRL explizit hin.

Links und Suchmaschinen sind für das Internet und das Auffinden von Informationen innerhalb der Vielzahl an Informationen unerlässlich. Es sind daher klare gesetzliche Regelungen erforderlich, die insbesondere den Suchmaschinenanbietern ausreichend Rechtssicherheit bringen, um sie in ihrem Geschäftsbetrieb nicht unnötig zu behindern.

Da sowohl der Linksetzer als auch der Suchmaschinenanbieter die Inhalte nicht originär im Internet zur Verfügung stellen, ist auch deren Inanspruchnahme entsprechend subsidiär auszugestalten.

Zu unterscheiden ist grundsätzlich zwischen dem Suchmaschinenanbieter und dem einfachen Setzen eines Hyperlinks. Während der Tätigkeit der Suchmaschine ein automatisierter technischer Vorgang zugrunde liegt, durch den eine große Anzahl von Inhalten indexiert wird, erfolgt das Setzen eines Hyperlinks in der Regel manuell, beispielsweise um im Rahmen des eigenen Internetauftritts auf weitere Webseiten zu verweisen. Zu unterscheiden ist insoweit auch das eigene Linksetzen des Webseitenbetreibers oder das Linksetzen eines Dritten auf einer fremden Webseite.

aa) Suchmaschinenanbieter

Grundsätzlich sind verschiedene Konstruktionen einer gesetzlichen Haftungsprivilegierung des Suchmaschinenanbieters denkbar.

Insbesondere von Seiten der Internetindustrie wird zunehmend eine Privilegierung analog der des Access-Providers gefordert.[1938]

[1938] Siehe bspw. eco, Stellungnahme zur Anbieterhaftung, S. 7; Google,

Begründet wird dies damit, dass der Suchmaschinenanbieter lediglich eine technische Infrastruktur zur Verfügung stelle und entsprechend auch weite Haftungsprivilegierung verdiene. Auch das Österreichische E-Commerce-Gesetz (ECG) sieht eine entsprechende Privilegierung analog der des Access-Providers vor.[1939]

Vorzugswürdig erscheint im Hinblick auf die Interessen der Urheberrechtsinhaber jedoch eine Regelung analog der des Host-Providers mit entsprechendem *Notice and Takedown*-Verfahren nach dem US-amerikanischen Modell. Das Hauptproblem am *Notice and Takedown*-Verfahren für den Suchmaschinenanbieter liegt darin, dass der Nutzer hier keine hinreichende Möglichkeit erhält, sich gegen die Entfernung seines Links aus den Suchmaschinenergebnissen zu verteidigen. Der Suchmaschinenanbieter steht in keinem vertraglichen Verhältnis mit dem Inhalteanbieter, weshalb neben dem praktischen Problem, dass ihm die Identität oftmals nicht bekannt ist, eine entsprechende Nachforschungs- und Informationspflicht durch den Suchmaschinenanbieter aufgrund der fehlenden Nähe zum Inhalteanbieter nicht zuzumuten ist. Dies birgt nicht lediglich die Gefahr, dass die Interessen der Inhalteanbieter und Nutzer nicht ausreichend berücksichtigt werden, sondern zudem, dass vermehrt unberechtigte oder zumindest fragwürdige Hinweise gesendet werden und dem Suchmaschinenanbieter hierdurch eine erheblicher Verwaltungsmehraufwand entsteht. Um diesem Problem entgegenzutreten, sollte der Hinweis Angaben über den dem Anspruch auf Entfernung der Verlinkung zugrundeliegenden Anspruch enthalten. Zudem sieht sich der Absender des Hinweises

---

Stellungnahme zur Anbieterhaftung, S. 25; zustimmend auch Holznagel, S. 241.

[1939] § 14 ECG: „*(1) Ein Diensteanbieter, der Nutzern eine Suchmaschine oder andere elektronische Hilfsmittel zur Suche nach fremden Informationen bereitstellt, ist für die abgefragten Informationen nicht verantwortlich, sofern er*
1. die Übermittlung der abgefragten Informationen nicht veranlasst,
2. den Empfänger der abgefragten Informationen nicht auswählt und
3. die abgefragten Informationen weder auswählt noch verändert.
(2) Abs. 1 ist nicht anzuwenden, wenn die Person, von der die abgefragten Informationen stammen, dem Diensteanbieter untersteht oder von ihm beaufsichtigt wird.“

aufgrund der Bezugnahme auf die Haftung für falsche Angaben Schadensersatzansprüchen ausgesetzt, sofern er nicht in gutem Glauben handelt. Durch die genauen Vorgaben an den Hinweis, erlangt der Suchmaschinenanbieter das erforderliche Maß an Rechtssicherheit für die Ausführung seiner Tätigkeit.

Da der Suchmaschinenanbieter zudem lediglich auf Inhalte verweist, die sich an anderer Stelle im Internet befinden, sollte seine Verpflichtung zum *takedown* gegenüber derjenigen des Host-Providers subsidiär ausgestaltet werden.

bb) Hyperlinks

Auch wenn das manuelle Setzen von Hyperlinks gegenüber dem automatischen Verfahren der Suchmaschinenanbieter gewisse Unterschiede aufweist, bietet sich dennoch eine gleiche Behandlung hinsichtlich der Voraussetzungen zur Haftungsprivilegierung an. Denn auch beim manuellen Linksetzen ist ein etwaig rechtsverletzender Inhalt nicht immer ohne Weiteres auf den ersten Blick erkennbar. Daher kann auch hier auf das *Notice and Takedown*-Verfahren des Suchmaschinenanbieters zurückgegriffen werden. Auch nach aktueller Rechtsprechung sieht der BGH eine Störerhaftung aufgrund der Verletzung von Prüfpflichten i.d.R. nur dann als gegeben an, wenn der Linksetzende Kenntnis von der Rechtsverletzung hatte oder haben musste.[1940]

Die gesetzliche Haftungsprivilegierung sollte entsprechend an die fehlende Kenntnis bzw. das fehlende Kennenmüssen anknüpfen und zusätzlich noch einen entsprechenden Hinweis nach den gesetzlichen Vorgaben mit einbeziehen.

Hinsichtlich Webseiten, auf denen nicht der Webseiten-Betreiber selbst die Links einstellt, sondern die Nutzer seiner Seite, ist auf die Bestimmungen zur Verantwortlichkeit des Host-Providers zurückzugreifen. Denn der Webseiten-Betreiber stellt hier lediglich die Plattform für die Inhalte Dritter bereit. Sofern Dritte Links zu urheberrechtsverletzenden Inhalten einstellen, hängt die Haftung

[1940] Siehe hierzu S. 185.

des Webseiten-Betreibers von seiner Kenntnis i.S.d. § 10 TMG ab. Hinsichtlich solcher Webseiten, dessen gesamtes Geschäftsmodell darin besteht, dass Dritte dort Links zu urheberrechtsverletzenden Inhalten einstellen, dürfte insoweit bereits nicht die Privilegierung greifen, da diesem in der Regel eine aktive Rolle zukommt, die ihm eine Kontrolle über die Inhalte verschafft.

4. Mögliche Kritikpunkte

Es ist absehbar, dass die hier vorgeschlagenen Lösungsansätze zur Schaffung von mehr Rechtssicherheit Kritik hervorrufen. Zu den wahrscheinlichsten Kritikpunkten wird im Folgenden bereits Stellung genommen.

a) Anwendung der Privilegien auf Unterlassungsansprüche

Die Anwendbarkeit der Privilegien auf Unterlassungsansprüche ist bereits seit langem Teil der im Schrifttum geführten Diskussion. Es ist abzusehen, dass die Anhänger eine Nichtanwendbarkeit der Privilegien auf Unterlassungsansprüche eine Unvereinbarkeit mit europäischen Vorgaben geltend machen werden. Hauptgrund für eine derartige Auslegung wird sein, dass der ISP als *Gatekeeper* und *Cheapest Cost Avoider* am besten in der Lage ist, effektiv Urheberrechtsverletzungen abzustellen. Zum Schutz der Rechte des geistigen Eigentums sei es daher geboten, diesem in einem gewissen Umfang auch Prüfpflichten zur Verhinderung zukünftiger Rechtsverletzungen aufzuerlegen.

Dem lässt sich aber entgegensetzen, dass der Schutz der Urheberrechte nicht schrankenlos zu gewähren ist. Vielmehr bedarf es einer Abwägung aller widerstreitenden Interessen, weshalb auch den Rechten der ISP und der Nutzer hinreichend Rechnung getragen werden muss. Daher ist auch eine Beurteilung nach dem *Cheapest Cost Avoider* als rein ökonomischer Ansatz ungeeignet, dieses Interessengeflecht der beteiligten Akteure vollständig abzubilden.[1941]

[1941] So auch Nolte/Wimmers, GRUR-Beilage 2014, 58, 60.

Soweit geltend gemacht wird, dass die Anwendbarkeit der Privilegien auf Unterlassungsansprüche gegen europäische Vorgaben verstößt, kann auf den Wortlaut der einschlägigen Bestimmungen der ECRL sowie der InfoSoc-RL verwiesen werden, wonach lediglich gerichtliche Anordnungen gegen die ISP unabhängig von einer Verantwortlichkeit ermöglicht werden müssen. Dieser Möglichkeit wird durch das diesseitige Lösungsmodell ausreichend Rechnung getragen. Insoweit ist es auch interessengerecht, eine entsprechende Anordnung lediglich auf die Entfernung/Sperrung des spezifischen Inhaltes zu begrenzen und keine weitergehende Unterlassungsverpflichtung hinsichtlich kerngleicher Verletzungen zu begründen. Denn eine solche Verpflichtung würde gegen das Verbot allgemeiner Überwachungspflichten verstoßen und ist auch nach der Rechtsprechung des EuGH abzulehnen.

Zudem kann erwartet werden, dass dem diesseitig vorgeschlagenen Lösungsmodell hinsichtlich des Host- und Cache-Providers sowie des Linksetzenden entgegengebracht wird, dass die Privilegien keine haftungsbegründende Norm darstellen, sondern lediglich Regelungen für einen Haftungsausschluss beinhalten.[1942] An dieser grundsätzlichen Funktion der Privilegien wird jedoch durch den diesseitig formulierten Vorschlag nicht gerüttelt. Dass bspw. der Host-Provider, nachdem er Kenntnis von einer Rechtsverletzung erlangt hat und diese nicht entfernt bzw. sperrt, als Störer auf Unterlassung haftet, leitet sich nicht aus dem in § 10 TMG formulierten Versäumnis einer Entfernung bzw. Sperrung ab. Vielmehr führt ein entsprechendes Versäumnis dazu, dass die Privilegien gerade nicht mehr beansprucht werden können. Die Verantwortlichkeit richtet sich nun nach den allgemeinen Gesetzen. Die Störerhaftung begründet sich darin, dass der Host-Provider Kenntnis von einer spezifischen Rechtsverletzung hat und ihn deswegen eine diesbezügliche Prüfpflicht trifft, welche sich in der Entfernung bzw. Sperrung des rechtsverletzenden Inhaltes

[1942] Was insoweit auch korrekt ist, siehe bspw. Wiebe, WRP 2012, 1182, 1186.

niederschlägt. Ein Verstoß gegen diese Pflichtverletzung begründet den gegen ihn gerichteten Unterlassungsanspruch.
Zudem könnte gegen die Begrenzung der Prüfpflichten auf das Zumutbare im Sinne einer Kenntnis der §§ 9-11 TMG eingewandt werden, dass, für den Fall, dass ein Gericht den ISP nicht als Störer einordnet und daher einen Unterlassungsanspruch ablehnt, der Urheberrechtsinhaber schutzlos dasteht. Denkbar wäre daher eine unionsrechtswidrige Schutzrechtslücke, da Artikel 8 Abs. 3 InfoSoc-RL explizit bestimmt, dass die Mitgliedstaaten sicherstellen müssen, dass die Rechteinhaber gerichtliche Anordnungen gegen Vermittler beantragen können, deren Dienste von einem Dritten zur Verletzung eines Urheberrechts genutzt werden. Wenn nun aber der Host-Provider nicht gegen zumutbare Prüfpflichten verstoßen hat, in dem Sinne, dass die behauptete Rechtsverletzung nicht offensichtlich war, kann nach den allgemeinen Gesetzen auch kein Anspruch auf Beseitigung bzw. Unterlassung gegen ihn durchgesetzt werden. Dies ist allerdings auch nach dem derzeitig anwendbarem System der Störerhaftung der Fall.
Zudem wird hier verkannt, dass das erkennende Gericht im Rahmen der Prüfung der Verletzung zumutbarer Prüfpflichten, auch die dem Anspruch zugrundeliegende Rechtsverletzung prüft. Stellt das Gericht fest, dass zwar eine Rechtsverletzung vorliegt, der ISP diesbezüglich aber keine Prüfpflichten verletzt hat, so hat der ISP spätestens nach Urteilsverkündung die seine Haftung auslösende Kenntnis i.S.d. §§ 9-11 TMG, welche ihn dann nach dem hier vorgeschlagenen Lösungsmodell entsprechend auch zur Entfernung bzw. Sperrung verpflichtet.

b) Notice and Takedown-Verfahren

Zudem wird das *Notice and Takedown*-Verfahren sich die bereits des Öfteren zutage gebrachte Warnung vor der massenhaften Versendung unberechtigter oder zumindest fragwürdigere Hinweise gefallen lassen. Hiergegen kann jedoch eingewandt werden, dass auch nach derzeitiger Rechtslage kein ausreichender

Schutz vor unberechtigten Hinweisen besteht. Im Gegenteil, dadurch, dass es keinerlei gesetzliche Vorgaben hinsichtlich des Inhaltes eines solchen Hinweises gibt, besteht eine noch größere Gefahr, dass ISP Inhalte aufgrund nicht hinreichender Hinweise löschen. Durch die Einführung gesetzlicher Mindestvorgaben wird insoweit wenigstens sichergestellt, dass derjenige, der einen Hinweis über eine beanstandete Rechtsverletzung sendet, bestimmte Angaben hinsichtlich des geltend gemachten Anspruches macht und er sich durch die spezifische Regelung hinsichtlich einer Haftung für falsche Angaben darüber im Klaren ist, dass eine innerhalb des Hinweises vorsätzlich oder grob fahrlässig falsch gemachte Angabe, Konsequenzen nach sich ziehen kann. Das hier vorgeschlagene Modell ist daher geeignet, der massenhaften Versendung unberechtigter Hinweise über Rechtsverletzungen zumindest in gewissem Maße Einhalt zu gebieten.

5. Vorgeschlagene Gesetzesänderung

(Änderungen zu den bestehenden Regelungen des TMG sind kursiv hinterlegt)

§ 7 Allgemeine Grundsätze.

(1) Diensteanbieter sind für eigene Informationen, die sie zur Nutzung bereithalten, nach den allgemeinen Gesetzen verantwortlich.

(2) Diensteanbieter im Sinne der §§ 8 bis *11* sind nicht verpflichtet, die von ihnen übermittelten oder gespeicherten Informationen zu überwachen oder nach Umständen zu forschen, die auf eine rechtswidrige Tätigkeit hinweisen.

§ 8 Durchleitung von Informationen

(1) Diensteanbieter sind für fremde Informationen, die sie in einem Kommunikationsnetz übermitteln oder zu denen sie den Zugang zur Nutzung vermitteln, nicht verantwortlich, sofern sie

1. die Übermittlung nicht veranlasst,
2. den Adressaten der übermittelten Informationen nicht ausgewählt und
3. die übermittelten Informationen nicht ausgewählt oder verändert haben.

Satz 1 findet keine Anwendung, wenn der Diensteanbieter absichtlich mit einem Nutzer seines Dienstes zusammenarbeitet, um rechtswidrige Handlungen zu begehen.

(2) Die Übermittlung von Informationen nach Absatz 1 und die Vermittlung des Zugangs zu ihnen umfasst auch die automatische kurzzeitige Zwischenspeicherung dieser Informationen, soweit dies nur zur Durchführung der Übermittlung im Kommunikationsnetz geschieht und die Informationen nicht länger gespeichert werden, als für die Übermittlung üblicherweise erforderlich ist.

(3) Der durch eine fremde Information in seinen Rechten Verletzte kann den Diensteanbieter auf Sperrung des Zugangs zu der Information in Anspruch nehmen, sofern eine vorherige Inanspruchnahme des unmittelbaren Rechtsverletzers oder anderer an der Rechtsverletzung beteiligter Diensteanbieter erfolglos blieb. Für die Erteilung der Sperrung ist eine vorherige richterliche Anordnung erforderlich. Für den Erlass einer entsprechenden Anordnung ist das Landgericht, in dessen Bezirk der zur Sperrung verpflichtete Diensteanbieter seinen Wohnsitz, seinen Sitz oder seine Niederlassung hat, ohne Rücksicht auf den Streitwert ausschließlich zuständig. Die Entscheidung trifft die Zivilkammer. Für das Verfahren gelten die Vorschriften des Gesetzes über das Verfahren in Familiensachen und in den Angelegenheiten der freiwilligen Gerichtsbarkeit entsprechend. Die Kosten der richterlichen Anordnung trägt der Verletzte. Gegen die Entscheidung des Landgerichts ist die Beschwerde statthaft. Die Beschwerde ist binnen einer Frist von zwei Wochen einzulegen.

§ 9 Zwischenspeicherung zur beschleunigten Übermittlung von Informationen

(1) Diensteanbieter sind für eine automatische, zeitlich begrenzte Zwischenspeicherung, die allein dem Zweck dient, die Übermittlung fremder Informationen an andere Nutzer auf deren Anfrage effizienter zu gestalten, nicht verantwortlich, sofern sie

1. die Informationen nicht verändern,
2. die Bedingungen für den Zugang zu den Informationen beachten,
3. die Regeln für die Aktualisierung der Informationen, die in weithin anerkannten und verwendeten Industriestandards festgelegt sind, beachten,
4. die erlaubte Anwendung von Technologien zur Sammlung von Daten über die Nutzung der Informationen, die in weithin anerkannten und verwendeten Industriestandards festgelegt sind, nicht beeinträchtigen und
5. unverzüglich handeln, um im Sinne dieser Vorschrift gespeicherte Informationen zu entfernen oder den Zugang zu ihnen zu sperren, sobald sie Kenntnis davon *oder einen Hinweis darüber erhalten* haben, dass die Informationen am ursprünglichen Ausgangsort der Übertragung aus dem Netz entfernt wurden oder der Zugang zu ihnen gesperrt wurde oder ein Gericht oder eine Verwaltungsbehörde die Entfernung oder Sperrung angeordnet hat.

§ 8 Abs. 1 Satz 2 gilt entsprechend.

(2) Sofern gespeicherte Informationen durch den Diensteanbieter aufgrund eines Hinweises entfernt oder der Zugang zu ihnen gesperrt werden soll, hat der Versender unter Angabe seiner Identität zu versichern hat, dass das streitgegenständliche Material auf der Ursprungsseite entfernt wurde bzw. eine Kopie der gerichtlichen oder verwaltungsbehördlichen Anordnung beizufügen.

§ 10 Speicherung von Informationen

(1) Diensteanbieter sind für fremde Informationen, die sie für einen

Nutzer speichern, nicht verantwortlich, sofern

1. sie keine Kenntnis von der rechtswidrigen Handlung oder der Information haben und ihnen im Falle von Schadensersatzansprüchen auch keine Tatsachen oder Umstände bekannt sind, aus denen die rechtswidrige Handlung oder die Information offensichtlich wird, oder

2. sie unverzüglich tätig geworden sind, um die Information zu entfernen oder den Zugang zu ihr zu sperren, sobald sie diese Kenntnis erlangt haben *oder einen Hinweis nach Vorgaben des Absatz 2 erhalten haben.*

Satz 1 findet keine Anwendung, wenn der Nutzer dem Diensteanbieter untersteht oder von ihm beaufsichtigt wird.

(2) Ein im Sinne des Absatz 1 Nummer 2 wirksamer Hinweis muss die folgenden Angaben enthalten:

1. Angaben zur Identität des Absenders inklusive Angaben zur telefonischen oder elektronischen Kontaktaufnahme,

2. Angaben zur beanstandeten rechtswidrigen Handlung oder Information inklusive der genauen Fundstelle, z.B. durch Angabe der URL und

3. Angaben über den der geforderten Entfernung oder Sperrung zugrundeliegenden Anspruch.

Der Hinweis ist an die von dem Diensteanbieter gemäß § 5 Satz 1 Nummer 2 zur Verfügung gestellte Adresse der elektronischen Post zu senden. Dem Diensteanbieter bleibt es unbenommen eine eigens für die Zusendung von Hinweisen nach Absatz 1 Satz 2 angelegte Adresse der elektronischen Post zu bestimmen und diese seinen Nutzern mitzuteilen.

(3) Nach Erhalt des Hinweises gemäß Absatz 2 hat der Diensteanbieter dem Nutzer unverzüglich eine Kopie des Hinweises zukommen zu lassen.

(4) Der Nutzer hat nach Erhalt des Hinweises die Möglichkeit dem Diensteanbieter eine Gegendarstellung zuzusenden. Die Gegendarstellung muss die folgenden Angaben enthalten:
1. Angaben zur Information welche aufgrund des Hinweises entfernt oder der Zugang zu ihr gesperrt wurde und
2. Angaben hinsichtlich der Unbegründetheit des in dem Hinweis geltend gemachten Anspruchs.

(5) Nach Erhalt einer Gegendarstellung gemäß Absatz 4 hat der Diensteanbieter die Entfernung oder Sperrung der Information unverzüglich aufzuheben und dem Absender des Hinweises unverzüglich eine Kopie der Gegendarstellung zukommen zu lassen. Personenbezogene Daten sind vom Diensteanbieter zu anonymisieren.

(6) Der Diensteanbieter ist nicht verantwortlich für die Entfernung oder Sperrung fremder Informationen aufgrund eines Hinweises gemäß Absatz 2 oder die Aufhebung der Entfernung oder Sperrung aufgrund einer Gegendarstellung gemäß Absatz 4.

(7) Für vorsätzlich oder grob fahrlässig gemachte falsche Angaben innerhalb des Hinweises gemäß Absatz 2 Nummer 3 oder der Gegendarstellung gemäß Absatz 4 Nummer 2 haftet der Absender des Hinweises oder der Gegendarstellung für den hierdurch bei der jeweils anderen Partei entstandenen Schaden.

(8) Hinweise, die nicht den Anforderungen des Absatz 2 und Gegendarstellungen, die nicht den Anforderungen des Absatz 4 entsprechen, kann der Diensteanbieter unbeachtet lassen.

§ 11 Verlinkungen zu Informationen

(1) Diensteanbieter, die Nutzern eine Suchmaschine zur Suche nach fremden Informationen bereitstellen, welche Links auf fremde Informationen generiert oder die auf fremde Informationen

verlinken, sind für diese fremden Informationen nicht verantwortlich, sofern
1. sie keine Kenntnis von der rechtswidrigen Handlung oder der Information haben und ihnen im Falle von Schadensersatzansprüchen auch keine Tatsachen oder Umstände bekannt sind, aus denen die rechtswidrige Handlung oder die Information offensichtlich wird, oder
2. sie unverzüglich tätig geworden sind, um die Verlinkung zu der Information zu entfernen oder den Zugang zu ihr zu sperren, sobald sie diese Kenntnis erlangt haben oder einen Hinweis gemäß § 10 Absatz 2 erhalten haben.
Satz 1 findet keine Anwendung, wenn der Nutzer dem Diensteanbieter untersteht oder von ihm beaufsichtigt wird.

(2) In Abänderung der gemäß § 10 Absatz 2 erforderlichen Angaben, sind anstelle der Angaben zur beanstandeten rechtswidrigen Handlung oder Information Angaben zu der Verlinkung zu machen, inklusive einer genauen Fundstelle der Verlinkung. Zusätzlich zu den in § 10 Absatz 2 genannten Angaben, hat der Versender des Hinweises zu versichern, dass er zuvor erfolglos einen entsprechenden Hinweis an den Diensteanbieter, der die Information auf die verlinkt wird speichert, gesendet hat.

(3) Der Nutzer des Diensteanbieters kann, nachdem er Kenntnis über die Entfernung der Verlinkung zu der Information oder der Sperrung des Zugangs zu der Verlinkung erlangt hat, von dem Diensteanbieter die Zusendung des Hinweises gemäß § 10 Absatz 2 verlangen.

(3) § 10 Absätze 4 bis 8 gelten entsprechend.

6. Ausblick

Die Verantwortlichkeit und Privilegierung der ISP wird auch in Zukunft die Gerichte beschäftigen. Wie die vorliegende

Untersuchung gezeigt hat, ist es für die ISP von besonderer Bedeutung, dass die Privilegien des TMG konsequent auch auf Unterlassungsansprüche angewandt werden. Gegebenenfalls bedarf es hier eines Tätigwerden des Gesetzgebers.

Das derzeit beim EuGH anhängige Vorabentscheidungsverfahren verspricht Klarheit bezüglich einer Anwendbarkeit der Privilegien auf Unterlassungsansprüche der ISP.

Es bedarf zudem weiterer Forschung, ob dass in dieser Arbeit vorgeschlagene Lösungsmodell, welches auf die Verletzung und Durchsetzung von Urheberrechten zugeschnitten ist, rechtsgebietsübergreifend angewandt werden kann. Es ist nicht auszuschließen, dass eine Einheitslösung nicht gangbar ist und hier bspw. eine Unterscheidung zwischen zivilrechtlichen und strafrechtlichen Verstößen vorzugswürdig ist.[1943]

[1943] So bereits von Seiten der Digitale Gesellschaft e.V. im Rahmen der Konsultation der EU-Kommission zur Einführung eines europäischen *Notice and Takedown*-Systems, siehe Digitale Gesellschaft, Public Consultation, S. 8.

Anhang: Auszug des § 512 DMCA

(a) Transitory Digital Network Communications.
A service provider shall not be liable for monetary relief, or, except as provided in subsection (j), for injunctive or other equitable relief, for infringement of copyright by reason of the provider's transmitting, routing, or providing connections for, material through a system or network controlled or operated by or for the service provider, or by reason of the intermediate and transient storage of that material in the course of such transmitting, routing, or providing connections, if
(1) the transmission of the material was initiated by or at the direction of a person other than the service provider;
(2) the transmission, routing, provision of connections, or storage is carried out through an automatic technical process without selection of the material by the service provider;
(3) the service provider does not select the recipients of the material except as an automatic response to the request of another person;
(4) no copy of the material made by the service provider in the course of such intermediate or transient storage is maintained on the system or network in a manner ordinarily accessible to anyone other than anticipated recipients, and no such copy is maintained on the system or network in a manner ordinarily accessible to such anticipated recipients for a longer period than is reasonably necessary for the transmission, routing, or provision of connections; and
(5) the material is transmitted through the system or network without modification of its content.

(b) System Caching.
(1) Limitation on liability.
A service provider shall not be liable for monetary relief, or, except as provided in subsection (j), for injunctive or other equitable relief, for infringement of copyright by reason of the intermediate and temporary storage of material on a system or network controlled or operated by or for the service provider in a case in which
(A) the material is made available online by a person other than the service provider;
(B) the material is transmitted from the person described in subparagraph (A) through the system or network to a person other than the person described in subparagraph (A) at the direction of that other person; and
(C) the storage is carried out through an automatic technical process for the purpose of making the material available to users of the system or network who, after the material is transmitted as described in subparagraph (B), request access to the material from the person described in subparagraph (A),
if the conditions set forth in paragraph (2) are met.
(2) Conditions.

The conditions referred to in paragraph (1) are that
(A) the material described in paragraph (1) is transmitted to the subsequent users described in paragraph (1)(C) without modification to its content from the manner in which the material was transmitted from the person described in paragraph (1)(A);
(B) the service provider described in paragraph (1) complies with rules concerning the refreshing, reloading, or other updating of the material when specified by the person making the material available online in accordance with a generally accepted industry standard data communications protocol for the system or network through which that person makes the material available, except that this subparagraph applies only if those rules are not used by the person described in paragraph (1)(A) to prevent or unreasonably impair the intermediate storage to which this subsection applies;
(C) the service provider does not interfere with the ability of technology associated with the material to return to the person described in paragraph (1)(A) the information that would have been available to that person if the material had been obtained by the subsequent users described in paragraph (1)(C) directly from that person, except that this subparagraph applies only if that technology
(i) does not significantly interfere with the performance of the provider's system or network or with the intermediate storage of the material;
(ii) is consistent with generally accepted industry standard communications protocols; and
(iii) does not extract information from the provider's system or network other than the information that would have been available to the person described in paragraph (1)(A) if the subsequent users had gained access to the material directly from that person;
(D) if the person described in paragraph (1)(A) has in effect a condition that a person must meet prior to having access to the material, such as a condition based on payment of a fee or provision of a password or other information, the service provider permits access to the stored material in significant part only to users of its system or network that have met those conditions and only in accordance with those conditions; and
(E) if the person described in paragraph (1)(A) makes that material available online without the authorization of the copyright owner of the material, the service provider responds expeditiously to remove, or disable access to, the material that is claimed to be infringing upon notification of claimed infringement as described in subsection (c)(3), except that this subparagraph applies only if
(i) the material has previously been removed from the originating site or access to it has been disabled, or a court has ordered that the material be removed from the originating site or that access to the material on the originating site be disabled; and
(ii) the party giving the notification includes in the notification a statement confirming that the material has been removed from the originating site or access to it has been disabled or that a court has ordered that the material be removed from the originating site or

that access to the material on the originating site be disabled.

(c) Information Residing on Systems or Networks At Direction of Users.

(1) In general.

A service provider shall not be liable for monetary relief, or, except as provided in subsection (j), for injunctive or other equitable relief, for infringement of copyright by reason of the storage at the direction of a user of material that resides on a system or network controlled or operated by or for the service provider, if the service provider

(A)

(i) does not have actual knowledge that the material or an activity using the material on the system or network is infringing;

(ii) in the absence of such actual knowledge, is not aware of facts or circumstances from which infringing activity is apparent; or

(iii) upon obtaining such knowledge or awareness, acts expeditiously to remove, or disable access to, the material;

(B) does not receive a financial benefit directly attributable to the infringing activity, in a case in which the service provider has the right and ability to control such activity; and

(C) upon notification of claimed infringement as described in paragraph (3), responds expeditiously to remove, or disable access to, the material that is claimed to be infringing or to be the subject of infringing activity.

(2) Designated agent.

The limitations on liability established in this subsection apply to a service provider only if the service provider has designated an agent to receive notifications of claimed infringement described in paragraph (3), by making available through its service, including on its website in a location accessible to the public, and by providing to the Copyright Office, substantially the following information:

(A) the name, address, phone number, and electronic mail address of the agent.

(B) other contact information which the Register of Copyrights may deem appropriate.

The Register of Copyrights shall maintain a current directory of agents available to the public for inspection, including through the Internet, and may require payment of a fee by service providers to cover the costs of maintaining the directory.

(3) Elements of notification.

(A) To be effective under this subsection, a notification of claimed infringement must be a written communication provided to the designated agent of a service provider that includes substantially the following:

(i) A physical or electronic signature of a person authorized to act on behalf of the owner of an exclusive right that is allegedly infringed.

(ii) Identification of the copyrighted work claimed to have been infringed, or, if multiple copyrighted works at a single online site

are covered by a single notification, a representative list of such works at that site.
(iii) Identification of the material that is claimed to be infringing or to be the subject of infringing activity and that is to be removed or access to which is to be disabled, and information reasonably sufficient to permit the service provider to locate the material.
(iv) Information reasonably sufficient to permit the service provider to contact the complaining party, such as an address, telephone number, and, if available, an electronic mail address at which the complaining party may be contacted.
(v) A statement that the complaining party has a good faith belief that use of the material in the manner complained of is not authorized by the copyright owner, its agent, or the law.
(vi) A statement that the information in the notification is accurate, and under penalty of perjury, that the complaining party is authorized to act on behalf of the owner of an exclusive right that is allegedly infringed.
(B)
(i) Subject to clause (ii), a notification from a copyright owner or from a person authorized to act on behalf of the copyright owner that fails to comply substantially with the provisions of subparagraph (A) shall not be considered under paragraph (1)(A) in determining whether a service provider has actual knowledge or is aware of facts or circumstances from which infringing activity is apparent.
(ii) In a case in which the notification that is provided to the service provider's designated agent fails to comply substantially with all the provisions of subparagraph (A) but substantially complies with clauses (ii), (iii), and (iv) of subparagraph (A), clause (i) of this subparagraph applies only if the service provider promptly attempts to contact the person making the notification or takes other reasonable steps to assist in the receipt of notification that substantially complies with all the provisions of subparagraph (A).

(d) Information Location Tools.
A service provider shall not be liable for monetary relief, or, except as provided in subsection (j), for injunctive or other equitable relief, for infringement of copyright by reason of the provider referring or linking users to an online location containing infringing material or infringing activity, by using information location tools, including a directory, index, reference, pointer, or hypertext link, if the service provider
(1)
(A) does not have actual knowledge that the material or activity is infringing;
(B) in the absence of such actual knowledge, is not aware of facts or circumstances from which infringing activity is apparent; or
(C) upon obtaining such knowledge or awareness, acts expeditiously to remove, or disable access to, the material;
(2) does not receive a financial benefit directly attributable to the infringing activity, in a case in which the service provider has the

right and ability to control such activity; and
(3) upon notification of claimed infringement as described in subsection (c)(3), responds expeditiously to remove, or disable access to, the material that is claimed to be infringing or to be the subject of infringing activity, except that, for purposes of this paragraph, the information described in subsection (c)(3)(A)(iii) shall be identification of the reference or link, to material or activity claimed to be infringing, that is to be removed or access to which is to be disabled, and information reasonably sufficient to permit the service provider to locate that reference or link.

(e) [...]

(f) Misrepresentations.
Any person who knowingly materially misrepresents under this section
(1) that material or activity is infringing, or
(2) that material or activity was removed or disabled by mistake or misidentification,
shall be liable for any damages, including costs and attorneys' fees, incurred by the alleged infringer, by any copyright owner or copyright owner's authorized licensee, or by a service provider, who is injured by such misrepresentation, as the result of the service provider relying upon such misrepresentation in removing or disabling access to the material or activity claimed to be infringing, or in replacing the removed material or ceasing to disable access to it.

(g) Replacement of Removed or Disabled Material and Limitation on Other Liability.
(1) No liability for taking down generally.
Subject to paragraph (2), a service provider shall not be liable to any person for any claim based on the service provider's good faith disabling of access to, or removal of, material or activity claimed to be infringing or based on facts or circumstances from which infringing activity is apparent, regardless of whether the material or activity is ultimately determined to be infringing.
(2) Exception.
Paragraph (1) shall not apply with respect to material residing at the direction of a subscriber of the service provider on a system or network controlled or operated by or for the service provider that is removed, or to which access is disabled by the service provider, pursuant to a notice provided under subsection (c)(1)(C), unless the service provider
(A) takes reasonable steps promptly to notify the subscriber that it has removed or disabled access to the material;
(B) upon receipt of a counter notification described in paragraph (3), promptly provides the person who provided the notification under subsection (c)(1)(C) with a copy of the counter notification, and informs that person that it will replace the removed material or cease disabling access to it in 10 business days; and

(C) replaces the removed material and ceases disabling access to it not less than 10, nor more than 14, business days following receipt of the counter notice, unless its designated agent first receives notice from the person who submitted the notification under subsection (c)(1)(C) that such person has filed an action seeking a court order to restrain the subscriber from engaging in infringing activity relating to the material on the service provider's system or network.

(3) Contents of counter notification.

To be effective under this subsection, a counter notification must be a written communication provided to the service provider's designated agent that includes substantially the following:

(A) A physical or electronic signature of the subscriber.

(B) Identification of the material that has been removed or to which access has been disabled and the location at which the material appeared before it was removed or access to it was disabled.

(C) A statement under penalty of perjury that the subscriber has a good faith belief that the material was removed or disabled as a result of mistake or misidentification of the material to be removed or disabled.

(D) The subscriber's name, address, and telephone number, and a statement that the subscriber consents to the jurisdiction of Federal District Court for the judicial district in which the address is located, or if the subscriber's address is outside of the United States, for any judicial district in which the service provider may be found, and that the subscriber will accept service of process from the person who provided notification under subsection (c)(1)(C) or an agent of such person.

(4) Limitation on other liability.

A service provider's compliance with paragraph (2) shall not subject the service provider to liability for copyright infringement with respect to the material identified in the notice provided under subsection (c)(1)(C).

(h) Subpoena To Identify Infringer.

(1) Request.

A copyright owner or a person authorized to act on the owner's behalf may request the clerk of any United States district court to issue a subpoena to a service provider for identification of an alleged infringer in accordance with this subsection.

(2) Contents of request.

The request may be made by filing with the clerk

(A) a copy of a notification described in subsection (c)(3)(A);

(B) a proposed subpoena; and

(C) a sworn declaration to the effect that the purpose for which the subpoena is sought is to obtain the identity of an alleged infringer and that such information will only be used for the purpose of protecting rights under this title.

(3) Contents of subpoena.

The subpoena shall authorize and order the service provider receiving the notification and the subpoena to expeditiously

disclose to the copyright owner or person authorized by the copyright owner information sufficient to identify the alleged infringer of the material described in the notification to the extent such information is available to the service provider.

(4) Basis for granting subpoena.

If the notification filed satisfies the provisions of subsection (c)(3)(A), the proposed subpoena is in proper form, and the accompanying declaration is properly executed, the clerk shall expeditiously issue and sign the proposed subpoena and return it to the requester for delivery to the service provider.

(5) Actions of service provider receiving subpoena.

Upon receipt of the issued subpoena, either accompanying or subsequent to the receipt of a notification described in subsection (c)(3)(A), the service provider shall expeditiously disclose to the copyright owner or person authorized by the copyright owner the information required by the subpoena, notwithstanding any other provision of law and regardless of whether the service provider responds to the notification.

(6) Rules applicable to subpoena.

Unless otherwise provided by this section or by applicable rules of the court, the procedure for issuance and delivery of the subpoena, and the remedies for noncompliance with the subpoena, shall be governed to the greatest extent practicable by those provisions of the Federal Rules of Civil Procedure governing the issuance, service, and enforcement of a subpoena duces tecum.

(i) Conditions for Eligibility.

(1) Accommodation of technology.

The limitations on liability established by this section shall apply to a service provider only if the service provider

(A) has adopted and reasonably implemented, and informs subscribers and account holders of the service provider's system or network of, a policy that provides for the termination in appropriate circumstances of subscribers and account holders of the service provider's system or network who are repeat infringers; and

(B) accommodates and does not interfere with standard technical measures.

(2) Definition.

As used in this subsection, the term "standard technical measures" means technical measures that are used by copyright owners to identify or protect copyrighted works and

(A) have been developed pursuant to a broad consensus of copyright owners and service providers in an open, fair, voluntary, multi-industry standards process;

(B) are available to any person on reasonable and nondiscriminatory terms; and

(C) do not impose substantial costs on service providers or substantial burdens on their systems or networks.

(j) Injunctions.

The following rules shall apply in the case of any application for an

injunction under section 502 against a service provider that is not subject to monetary remedies under this section:

(1) Scope of relief.

(A) With respect to conduct other than that which qualifies for the limitation on remedies set forth in subsection (a), the court may grant injunctive relief with respect to a service provider only in one or more of the following forms:

(i) An order restraining the service provider from providing access to infringing material or activity residing at a particular online site on the provider's system or network.

(ii) An order restraining the service provider from providing access to a subscriber or account holder of the service provider's system or network who is engaging in infringing activity and is identified in the order, by terminating the accounts of the subscriber or account holder that are specified in the order.

(iii) Such other injunctive relief as the court may consider necessary to prevent or restrain infringement of copyrighted material specified in the order of the court at a particular online location, if such relief is the least burdensome to the service provider among the forms of relief comparably effective for that purpose.

(B) If the service provider qualifies for the limitation on remedies described in subsection (a), the court may only grant injunctive relief in one or both of the following forms:

(i) An order restraining the service provider from providing access to a subscriber or account holder of the service provider's system or network who is using the provider's service to engage in infringing activity and is identified in the order, by terminating the accounts of the subscriber or account holder that are specified in the order.

(ii) An order restraining the service provider from providing access, by taking reasonable steps specified in the order to block access, to a specific, identified, online location outside the United States.

(2) Considerations.

The court, in considering the relevant criteria for injunctive relief under applicable law, shall consider—

(A) whether such an injunction, either alone or in combination with other such injunctions issued against the same service provider under this subsection, would significantly burden either the provider or the operation of the provider's system or network;

(B) the magnitude of the harm likely to be suffered by the copyright owner in the digital network environment if steps are not taken to prevent or restrain the infringement;

(C) whether implementation of such an injunction would be technically feasible and effective, and would not interfere with access to noninfringing material at other online locations; and

(D) whether other less burdensome and comparably effective means of preventing or restraining access to the infringing material are available.

(3) Notice and ex parte orders.

Injunctive relief under this subsection shall be available only after notice to the service provider and an opportunity for the service provider to appear are provided, except for orders ensuring the preservation of evidence or other orders having no material adverse effect on the operation of the service provider's communications network.

(k) Definitions.
(1) Service provider.
(A) As used in subsection (a), the term "service provider" means an entity offering the transmission, routing, or providing of connections for digital online communications, between or among points specified by a user, of material of the user's choosing, without modification to the content of the material as sent or received.
(B) As used in this section, other than subsection (a), the term "service provider" means a provider of online services or network access, or the operator of facilities therefor, and includes an entity described in subparagraph (A).
(2) Monetary relief.
As used in this section, the term "monetary relief" means damages, costs, attorneys' fees, and any other form of monetary payment.
(l) Other Defenses Not Affected.
The failure of a service provider's conduct to qualify for limitation of liability under this section shall not bear adversely upon the consideration of a defense by the service provider that the service provider's conduct is not infringing under this title or any other defense.

(m) Protection of Privacy.
Nothing in this section shall be construed to condition the applicability of subsections (a) through (d) on
(1) a service provider monitoring its service or affirmatively seeking facts indicating infringing activity, except to the extent consistent with a standard technical measure complying with the provisions of subsection (i); or
(2) a service provider gaining access to, removing, or disabling access to material in cases in which such conduct is prohibited by law.

(n) Construction.
Subsections (a), (b), (c), and (d) describe separate and distinct functions for purposes of applying this section. Whether a service provider qualifies for the limitation on liability in any one of those subsections shall be based solely on the criteria in that subsection, and shall not affect a determination of whether that service provider qualifies for the limitations on liability under any other such subsection.

Lebenslauf:

Persönliche Daten

Name	Rilana Wenske

Beruflicher Werdegang

05/2016 – 12/2016	**DLA Piper UK LLP, München** Transaction Lawyer
09/2015 - 04/2016	**DLA Piper UK LLP, München** Wissenschaftliche Mitarbeiterin
02/2014 - 12/2014	**cleverbridge AG, Köln** Legal Assistant
08/2013 - 12/2014	**Willers Müller-Römer Kunze & Partner, Köln** Wissenschaftliche Mitarbeiterin
01/2011 - 12/2012	**GRUNDY Light Entertainment GmbH, Köln** Justiziarin

Akademische Ausbildung

08/2013 – 12/2016	**Universität zu Köln** Promotionsstudium an der Rechtswissenschaftlichen Fakultät
01/2015 - 07/2015	**University of California, Berkeley** Visiting Researcher, School of Law
01/2009 - 01/2010	**Stockholms Universitet** Master of European Intellectual Property Law, Abschluss: Master of Laws (One Year), LL.M.
07/2006 - 12/2006	**University of Technology, Sydney** Auslandssemester
09/2004 - 07/2008	**Hochschule Darmstadt** Studiengang: Informationsrecht, Abschluss: „Diplom-Informationsjuristin (FH)“