

DANIEL HOLZNAGEL

*Notice and
Take-Down-Verfahren
als Teil der
Providerhaftung*

*Geistiges Eigentum und
Wettbewerbsrecht*

79

Mohr Siebeck

Daniel Holznagel

Notice and Take-Down-Verfahren als Teil der Providerhaftung

Untersuchung des rechtlichen Rahmens von
Verfahren zur Beanstandung und Verteidigung
von Inhalten im Internet, insbesondere auf „User
Generated Content“-Plattformen



Mohr Siebeck

Daniel Holznagel, geboren 1979; Studium Rechtswissenschaften Berlin (HU+FU); BIT-KOM (Bereich IT/IP/TK-Recht); Referendariat in Berlin, Bonn und San Francisco, seit 2010 Richter in Berlin.

ISBN 978-3-16-152667-1

ISSN 1860-7306 (Geistiges Eigentum und Wettbewerbsrecht)

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliographie; detaillierte bibliographische Daten sind im Internet über <http://dnb.dnb.de> abrufbar.

© 2013 Mohr Siebeck Tübingen. www.mohr.de

Das Werk einschließlich aller seiner Teile ist urheberrechtlich geschützt. Jede Verwertung außerhalb der engen Grenzen des Urheberrechtsgesetzes ist ohne Zustimmung des Verlags unzulässig und strafbar. Das gilt insbesondere für Vervielfältigungen, Übersetzungen, Mikroverfilmungen und die Einspeicherung und Verarbeitung in elektronischen Systemen.

Das Buch wurde von Gulde-Druck in Tübingen auf alterungsbeständiges Werkdruckpapier gedruckt und von der Buchbinderei Nädle in Nehren gebunden.

Geistiges Eigentum und Wettbewerbsrecht

herausgegeben von

Peter Heermann, Diethelm Klippel,
Ansgar Ohly und Olaf Sosniza

79



Vorwort

Dissertationen im Internetrecht unterliegen einem ständigen Aktualisierungsdruck. Als ich im Jahr 2006 erstmals mit dem Thema *notice and take down* in Berührung kam, waren die Erwartungen groß, dass der deutsche Gesetzgeber tätig würde, um bei der Providerhaftung nachzujustieren und dass er sich dabei stärker am amerikanischen *notice and take down* Verfahren orientieren könnte. Diese Hoffnungen zerschlugen sich. Die Providerhaftung wurde ausschließlich von der Rechtsprechung fortentwickelt. Die als zum Teil zu providerfreundlich empfundenen Haftungsprivilegierungen in ECRL und TMG wurden dabei praktisch zurückgedrängt; ihr Wortlaut spielt heute fast keine Rolle mehr. Der eigentliche Ablauf der Meldung (und ggfs. Verteidigung) von strittigen Online-Inhalten bzw. die rechtliche Absicherung dieser Prozesse blieb dabei weitgehend ungeklärt.

Eine quasi gegenläufige Konsolidierung fand währenddessen in den USA statt. Die dortigen außerordentlich detailtiefen Haftungsprivilegierungen in § 512 U.S. Copyright Act, dessen Kernstück das sog. *notice and take-down* Verfahren ist, haben sich bewährt. Die amerikanischen Gerichte haben die meisten Fragen zum Meldeverfahren geklärt und sind dabei dem Gesetzeswortlaut treu geblieben. In den USA haben die Provider, insbesondere UGC-Dienste, inzwischen erstaunliche Rechtssicherheit für den Umgang mit Meldungen (*notices*) rechtswidriger Nutzerinhalte. Ähnliches gilt für den Umgang mit Protesten (*counter notices*) von Nutzern gegen die unter Umständen unberechtigte Entfernung ihrer Inhalte.

Der (späte) Zeitpunkt des Abschlusses der vorliegenden Arbeit erweist sich inzwischen als Glücksfall. Die amerikanische Regelung bietet umfangreiche und gesicherte Erkenntnisse zu *notice and take down*. Auf der anderen Seite mehren sich in Europa (wieder) die Anzeichen, dass der Gesetzgeber das Verfahren der Verdachtsmeldung (als einen Teilbereich der Providerhaftung) regeln könnte. Nach einer Konsultation im Jahre 2010 hat die EU-Kommission in 2012 eine Initiative zu „notice and action procedures“ beschlossen, die offenbar zu einer horizontalen Rahmenregelung für Melde- und Abhilfeverfahren beim Umgang mit rechtswidrigen Inhalten im Internet führen soll.

Die vorliegende Arbeit wurde im Sommersemester 2010 von der juristischen Fakultät der Georg-August-Universität zu Göttingen als Dissertation

angenommen. Die vorliegende Druckfassung befindet sich nun auf dem Stand 1.1.2013.

Mein großer Dank gilt Vielen, die zum Gelingen dieser Arbeit beigetragen haben. An erster Stelle ist mein Doktorvater, Prof. Dr. Gerald Spindler zu nennen. Seine klare Denkweise bei der Lösung juristischer Probleme, insbesondere bei der Providerhaftung, ist mir ein Vorbild. Danken möchte ich auch meinem Zweitgutachter, Prof. Dr. Andreas Wiebe, LL.M. Das Interesse an dem Thema hat mein früherer Kollege, Dr. Volker Kitz, LL.M., geweckt. Ich verdanke ihm, als auch meinem früheren Kollegen Dr. Guido Brinkel, wertvolle Hinweise in der Anfangsphase der Arbeit.

Vor allem aber danke ich meinen Eltern, Gisela und Burkhard Holznagel. Ohne ihre Unterstützung und ihren Ansporn wären sowohl die Promotion als auch meine gesamte Ausbildung nicht möglich gewesen. Besonders denke ich dabei an meinen Vater, der den erfolgreichen Abschluss der Dissertation nicht mehr erleben konnte. Ihm widme ich die vorliegende Arbeit.

Berlin im Februar 2013

Daniel Holznagel

Abkürzungsverzeichnis

Die verwendeten Abkürzungen ausländischer Literatur erklären sich aus dem Literaturverzeichnis. Neben den üblichen juristischen Abkürzungen verwendet die vorliegende Arbeit ferner spezielle Abkürzungen, die im Folgenden aufgeführt werden:

BPJM	Bundesprüfstelle für jugendgefährdende Medien
CDA	Communications Decency Act
DMCA	Digital Millennium Copyright Act
DRM	Digital Rights Management
ECRL	Richtlinie 2000/31/EG (E-Commerce-Richtlinie)
EFF.....	Electronic Frontier Foundation
EnforcementRL.....	Richtlinie 2004/48/EG
FSM	Freiwillige Selbstkontrolle Multimedia
H. R. Rep.	House of Representatives Report
InfoSocRL.....	Richtlinie 2001/29/EG (Urheberrechtsrichtlinie)
ISP	Internet Service Provider
NTD	Notice and take-down (-Verfahren)
P2P	peer-to-peer
S. Rep.	Senate Report
UGC	User generated content
U.S.C.	United States Code
VeRO	Verified Rights Owners (Programme)
WIPO	World Intellectual Property Organization
9th Circuit	Court of Appeals for the 9th Circuit (USA)

In der Arbeit wird mit „Provider“ oder „Diensteanbieter“ derjenige bezeichnet, der im breitesten Sinne Dienstleistungen und Infrastrukturen zur Nutzung des Internet durch Dritte bereit hält. Mit „Inhalteanbieter“ werden diese Dritten bezeichnet, die selbst Inhalte im Internet verbreiten oder Services der Provider nutzen. Teilweise wird hier auch der Begriff „Nutzer“ verwendet. Mit „Verdachtsmelder“ wiederum ist derjenige bezeichnet, der gegenüber einem Provider geltend macht, ein bestimmter Inhalt eines Dritten (Inhalteanbieters) sei unzulässig.

Inhaltsverzeichnis

Vorwort.....	V
Abkürzungsverzeichnis.....	XVI
§ 1 Einleitung.....	1
§ 2 USA.....	5
<i>A. Verantwortlichkeit im Urheberrecht</i>	5
I. Direct Infringement	6
II. Contributory Infringement	7
1. Contribution.....	8
2. Knowledge.....	9
a) actual knowledge.....	9
b) constructive knowledge.....	10
aa) Sony (substantial non-infringing use)	10
bb) Grokster (inducement)	11
III. Vicarious Infringement	12
1. declining to exercise a right to stop or limit.....	13
2. profiting from direct infringement.....	15
IV. Ausblick: Secondary Liability nach Grokster	17
<i>B. Entstehung von § 512</i>	18
I. Providerhaftung vor dem DMCA.....	19
II. Hintergrund der Gesetzesentstehung.....	21
<i>C. Notice and take-down in § 512</i>	23
I. Verhältnis zum Haftungsrecht.....	23
II. Voraussetzungen des safe harbour	25
1. Anwendungsbereich	25
2. Designated Agent	26

3. Die sog. „threshold requirements“	27
a) Repeat Infringer Policy	27
aa) Notices als Auslöser?	27
bb) reasonable implementation	28
cc) Information der Nutzer.....	30
dd) Anwendbarkeit für Hyperlinks?	30
ee) Zwischenergebnis.....	30
b) Standard Technical Measures	31
c) Kein „actual or apparent knowledge“	31
d) Kein „right and ability to control“ bei „direct financial benefit“	34
aa) right and ability to control.....	35
bb) direct financial benefit	37
e) Zwischenergebnis.....	39
4. Take-down nach vollständiger notice.....	39
a) Form	39
b) Identifizierung der eigenen Werke.....	40
c) Identifizierung der Rechtsverletzung (nicht: inhaltliche Begründung)	41
d) Sonstige Inhalte der notice	44
e) Unverzögerlicher take-down.....	44
f) Unvollständige notices	45
5. Exkurs: Kenntnisverschaffung durch notice?.....	46
6. Exkurs: vorbeugende notice?	47
III. Umfang und Reichweite der Haftungsprivilegierung	48
1. Injunctions	49
2. Versteckte Obliegenheit zum pro-aktiven Filtern?.....	51
a) Abschließende Pflichtenverteilung in § 512	52
b) Explizite Erwähnung von Monitoringpflichten und technischen Kontrollmaßnahmen.....	53
c) Restriktive Tendenz im Markenrecht.....	53
3. Haftungsfreistellung für „Infringement of Copyright“	54
IV. „Good samaritan“ Freistellung, counter notice & put-back	54
V. Auskunftsverfahren	57
VI. Unbegründete notices	58
1. Empirik	58
2. Schadensersatz bei unbegründeter notice	60
a) „Good faith“ und „misrepresentation“: subjektiver Standard	60
b) Ungenauigkeiten in der notice	61
c) Verkennung Rechtfertigungsgründe (v.a. fair use).....	62
d) Erstattungsfähiger Schaden.....	63
3. Zwischenergebnis	64

VII. Kritik, Änderungsvorschläge, Ausblick 65

1. Tendenz zum (ungeprüften) take-down..... 66
 - a) Einschränkung zulässiger Verhalten 67
 - b) Systemimmanente Missbrauchsanfälligkeit? 68
 - c) Grundsätzliche Alternativen? 70
2. Mangelnder Verfahrensschutz..... 70
 - a) Fehlende Aufklärung über counter-notice 71
 - b) Take-down vor Weiterleitung der notice 71
 - c) Keine Pflicht zum put-back..... 71
 - d) „down-time“ bis zum put-back 72
 - e) Prüfungspflicht des Providers? 72
3. Mangelnde Sanktionen? 72
4. „Repeat infringer“ Regelung 73
5. Suchmaschinen und NTD..... 73

§ 3 Klärung gesetzlicher NTD-Elemente am Beispiel
europäischer Regelungen 75

A. Regelung der Anforderungen an eine Verdachtsmeldung..... 76

B. Safe harbour bei Befolgen formal korrekter notice..... 78

C. Counter-notice & put-back 79

D. Sonstige regelbare Aspekte 81

- I. Anwendungsbereich 81
- II. Subsidiarität..... 81
- III. Sanktionierung unbegründeter Verdachtsmeldungen 81
- IV. Injunctions 82
- V. Verbot von Monitoringpflichten 82
- VI. Auskunftsansprüche 83
- VII. Freiwillige Kontrollen 83

§ 4 Übernationales Recht..... 84

A. Verantwortlichkeit der Vermittler vs. NTD 84

- I. Öffnung der ECRL für NTD 84
- II. Injunctions gegen Vermittler..... 86
- III. TRIPS 87

B. Free speech & public domain 88

C. Zwischenergebnis	88
D. Exkurs: Tätigwerden des EU-Gesetzgebers?	89
§ 5 Deutschland	93
A. Providerhaftung	93
I. Passivlegitimation: Rückgriff auf Kategorien des allg. Zivilrechts	94
1. Täter	95
a) Verkehrspflichten	96
b) „Zu eigen machen“ von Inhalten	98
c) „Mittelbarer“ Täter?	100
2. Anstifter und Gehilfen	100
3. Störer	102
4. Zwischenergebnis	103
II. Unterlassungs- und Beseitigungsansprüche	104
1. Verletzung geschützter Rechtsgüter oder Interessen durch Dritte ..	104
2. Verletzung von Prüfungs- bzw. Verkehrspflichten	104
3. Bestimmung der Prüfungs- bzw. Verkehrspflichten	106
a) Wirtschaftliche Zumutbarkeit	106
b) Schwere der Verstöße / betroffene Rechtsgüter	108
c) Grad der Veranlassung	108
d) Soziale Nützlichkeit, Grundrechtsrelevanz	109
4. Kritik, Entwicklungsperspektiven	109
a) Pro-aktive Unterlassungspflichten	109
b) Prüfungspflichten als Verkehrspflichten	112
c) Besonderheiten bei der Bestimmung der Verkehrspflichten	112
aa) Verbot allg. Monitoringpflichten	113
bb) Provider als „Gatekeeper“	113
cc) Schutzbedürftigkeit des Verletzten	114
dd) Grundrechtsrelevanz, Seiteneffekte	116
III. Schadensersatzansprüche	116
1. Bisherige Rechtsprechung	116
2. Verkehrspflichtenverletzung bzw. „zu eigen machen“	116
3. § 10 TMG	118
IV. Haftungsprivilegierungen in ECRL und TMG	119
1. Erfasste Verletzungshandlungen	119
2. Erfasste Rechtsfolgen gegen Provider	119
3. Erfasste Tätigkeiten	120
a) Durchleitung, Caching, Hosting	120
b) ECRL: nur „neutrale“ Provider	120

c) TMG: nur „fremde“ Inhalte	123
4. Unverzügliches Entfernen nach bestimmtem Kenntnislevel.....	123
5. Zwischenergebnis	124
V. Zwischenergebnis und Ausblick	125
B. NTD de lege lata.....	125
I. Verdachtsmeldung.....	126
1. Auslöser von Handlungsobliegenheiten.....	126
2. Abgrenzung zur Abmahnung	127
3. Handlungsobliegenheiten vor (ohne) Verdachtsmeldung	128
4. Rechtliche Einordnung	129
a) geschäftsähnliche Handlung	129
b) (Keine) Begründung einer Sonderbeziehung.....	130
5. Anforderungen an die Verdachtsmeldung.....	132
a) Form	132
b) Inhalt	133
aa) Identitäts- und Kontaktangaben	133
bb) Lokalisierung	134
cc) Inhaltliche Begründung.....	135
c) Verdachtsmelder	139
d) Verdachtsempfänger	140
6. Folgen (unzureichender) Verdachtsmeldungen.....	141
7. Rücknahme	143
8. Kosten.....	143
9. Zwischenergebnis	144
II. Haftung für take-downs im Innenverhältnis.....	144
1. Vertragspflichtverletzung	144
a) Vertragsbeziehung	144
b) Pflichtwidrigkeit.....	145
c) Exkurs: Durchsetzung des put-back.....	146
2. Verschulden	147
a) Verschuldensmaßstab.....	147
aa) § 599 BGB (analog) für „kostenlose“ Angebote?.....	147
(1) Unentgeltlichkeit.....	148
(2) Nutzung als Entgelt?	148
(3) Werbeaufmerksamkeit als Entgelt?.....	149
(4) Rechteeinräumung bzw. Datenüberlassung als Entgelt?	151
bb) § 101 Abs. 6 UrhG analog?	152
b) Erforderliche Sorgfalt beim take-down.....	152
aa) Host als Intermediär (Fremdheit der Inhalte).....	153
bb) Unaufklärbarkeit auch nach Einholung von Rechtsrat	153

cc) Drohende (unklare) Außenhaftung	154
c) Erforderliche Sorgfalt nach counter-notice	155
d) Erforderliche Sorgfalt bei gleichartigen Verletzungsfällen	156
3. Zwischenergebnis	157
4. Exkurs: gesetzliche Ansprüche	157
III. Sperrklauseln („good samaritan“ Regelung)	158
1. Vorbehalt der jederzeitigen Löschung	158
2. Verdachtsklauseln	160
a) Vorüberlegungen	160
b) Verdachtsgrad	162
c) Verfahren	163
d) Put-back	164
e) AGB-Kontrolle	165
aa) Überraschende Klauseln	165
bb) Haftungsausschluss, Kardinalspflichten	166
cc) Sonstige unangemessene Benachteiligung	167
dd) Exkurs: Abgrenzung zu anderen Sanktionen	168
3. Sperrerlaubnis bei „unzulässigen“ Inhalten	168
4. Exkurs: virtuelle Hausordnung	168
5. Zwischenergebnis	169
IV. Verantwortlichkeit des Verdachtsmelters	170
1. Vorüberlegung: Kooperatives Vorgehen	171
2. Negative Feststellungsklage	171
3. Materielle Ansprüche	172
a) Vergleichbarkeit mit Abnehmerverwarnung	172
aa) Ähnlichkeiten	174
(1) Missbrauchsanfälligkeit wegen Dreiecksbeziehung	175
(2) Einschneidende Folgen	176
(3) Notwendigkeit eines Korrelats zu Monopolrechten	178
bb) Unterschiede	180
(1) (Oft) Keine Geltendmachung von Ansprüchen	180
(2) Die Schutzrechte	180
(3) Bedürfnis nach Vorgehen gegen Mittelsperson	182
cc) Zwischenergebnis	182
b) Die Anspruchsgrundlagen	183
aa) § 823 Abs. 2 BGB	183
bb) § 824 BGB	183
(1) Tatsachenbehauptung	183
(2) Schädigungseignung	184
(3) Berechtigte Interessen	185
cc) § 826 BGB	186
(1) Sittenwidrigkeit bei der Schutzrechtsverwarnung	186

(2) Sittenwidrigkeit der Verdachtsmeldung.....	187
dd) § 3 Abs. 1 UWG	189
(1) Anwendungsbereich	189
(2) Aktivlegitimation	190
(3) Die Unlauterkeit der Verdachtsmeldung.....	190
ee) Geschäftsführung ohne Auftrag (GoA).....	191
(1) § 678 BGB.....	191
(2) §§ 683 S. 1, 670 BGB	193
ff) Zwischenergebnis: Schutzlücken?	193
gg) § 823 Abs. 1 BGB.....	194
(1) Rechtsbehauptungen Dritter als allgemeines Lebensrisiko.....	194
(2) Eingriff in das Recht am Gewerbebetrieb.....	195
(3) Eingriff in das Allgemeine Persönlichkeitsrecht.....	197
(4) Sorgfaltsmaßstab	199
(5) Mitverschulden.....	202
c) Rechtsfolgen und Prozessuales	203
aa) Abwehr von Tatsachenbehauptungen	203
bb) Abwehr von Werturteilen?	203
cc) Auskunft.....	204
dd) Schadensersatz.....	204
ee) Geldentschädigung bei Verletzung des APR	204
4. Exkurs: Ansprüche des Providers gegen den Verdachtsmelder	205
a) Irrtum über Passivlegitimation.....	205
b) Irrtum über unmittelbare Verletzung	206
5. Zwischenergebnis	206
V. (hier sog.) „Seiteneffekte“.....	206
1. Unberechtigte take-downs	208
a) Empirik.....	208
b) Gewerbliche und private Verdachtsmeldungen	211
c) Verschulden des Verdachtsmelders	211
aa) Rechtsirrtümer.....	212
bb) Tatsachenirrtümer	214
d) Motive des Verdachtsmelders.....	216
e) Zusammenhang zwischen Motiven und Irrtümern	216
2. Störung des immaterialgüterrechtlichen Gleichgewichts?	217
a) Begrenzung von Immaterialgüterrechten.....	217
b) Beispiel DRM: Privatisierung der Grenzziehung	219
c) Notice and take-down: Privatisierung der Grenzüberwachung	220
C. Überlegungen de lege ferenda	223
I. Verfassungsrechtliche Wertungen.....	223

1. Maßgebliche Vorgaben	224
a) Art. 5 GG.....	224
aa) Meinungsfreiheit	224
bb) Medienfreiheit.....	225
(1) Pressefreiheit	225
(2) Rundfunkfreiheit	227
(3) Einheitliche Medienfreiheit, Anwendungsbereich „im“ Internet	227
cc) Zensurverbot	229
dd) Informationsfreiheit	232
b) Weitere Grundrechte	232
2. Grundgesetz und Haftungsrecht	233
a) Haftung der traditionellen Medien.....	233
b) Providerhaftung.....	234
aa) §§ 7 – 10 TMG	234
bb) Prüfungs- bzw. Verkehrspflichten	235
c) „Good samaritan“ Regelung	236
d) Haftung des Verdachtsmelders	236
3. Staatlicher Schutzauftrag.....	236
II. Mögliche (gesetzliche) NTD-Elemente	239
1. Politische Diskussion.....	240
a) Suchmaschinen.....	241
b) Host-Provider	242
c) Subsidiarität	244
d) Besondere Zuständigkeiten für die „notice“	245
e) Zwischenergebnis.....	246
2. Gesetzliche NTD-Lösungen	246
a) Konkretisierung der Kenntnisvermittlung	246
aa) Mögliche Regelungen	246
bb) Bewertung.....	248
b) Ausschluss pro-aktiver Pflichten für „gute“ Provider.....	249
aa) Mögliche Regelung	249
bb) Bewertung.....	250
c) Notice and take-down (entsprechend § 512 U.S. Copyright Act)	250
aa) Mögliche Regelung	251
bb) Bewertung.....	252
d) Isoliertes „put-back“	252
aa) Mögliche Regelung	253
bb) Bewertung.....	254
(1) Seiteneffekte und Schutzauftrag	254
(2) Put-back als Erfolgsmodell	254

(3) Keine Lösung durch Selbstregulierung	255
cc) Exkurs: put-back ohne Verdachtsmelder (gleichartige Verletzungen)	257
e) Missbrauchssanktionen	258
aa) Verschuldenshaftung (ggfs. Beweislastumkehr)	258
bb) Gefährdungshaftung wie bei der Grenzbeschlagnahme? ...	259
f) Zwischenergebnis	260
III. Übertragung auf andere Sachverhalte	261
1. Datenherausgabe durch Provider	261
2. Quick-Freeze	261
3. „repeat infringer“ Regelungen (Olivienne, 3-Strikes-Out)	262
4. Bewertungen in Netzwerken (z.B. eBay)	263
§ 6 Schlussbetrachtung	264
A. Vertrauensvorschuss für den Verdachtsmelder	264
B. Anforderungen an die Verdachtsmeldung	265
C. Verbindung von NTD mit Haftungsfreistellungen	265
D. Missbrauchs- und Fehleranfälligkeit	266
E. Sanktionierung unbegründeter Verdachtsmeldungen	268
F. Put-back Verfahren	269
Anhang: § 512 U.S. Copyright Act (Auszug)	271
Literaturverzeichnis	279
Sachregister	293

§ 1 Einleitung

Die Verantwortlichkeit der Internetprovider für Rechtsverletzungen ihrer Nutzer ist ein kontrovers diskutiertes Thema. Jedes Haftungsregime muss beachten, dass die Provider ihre Dienste im Massenverkehr erbringen und meist nur wenig Bezug zur im Einzelfall beanstandeten Information oder Handlung haben. Werden die Internetprovider aufgefordert, ein konkretes Verhalten zu unterbinden bzw. einen konkreten Inhalt zu sperren, geraten sie dennoch in die Situation, letztlich über den Einzelfall entscheiden zu müssen (Richterrolle). Sie finden sich dann mitunter zwischen den eigentlich streitenden Parteien wieder (Rechteinhaber sowie Nutzer bzw. Inhabtanbieter). An dieser Stelle setzt *notice and take-down* (NTD) an. Ausgehend von der Einsicht, dass die Provider für diesen Streit „schlechte“ Entscheider sind, soll das Verfahren, wie die Parteien an den Provider herantreten können, geregelt werden. Im Idealfall wird dem Provider die „Richterrolle“ weitgehend abgenommen und die eigentlich streitenden Parteien werden aufeinander verwiesen. *Notice and take-down* regelt vor allem, wie der Rechteinhaber eine angebliche Rechtsverletzung gegenüber dem Provider geltend machen kann, welche Konsequenzen eine formal unzureichende oder inhaltlich unrichtige Verdachtsmeldung nach sich zieht und mit welcher Art von „Verteidigungsmeldung“ (*counter-notice*) der betroffene Nutzer seine Inhalte im Internet verteidigen kann. Um diese Verfahren (ob gesetzlich ausgestaltet oder nicht) geht es in vorliegender Arbeit.

Nicht für alle Provider bzw. Diensteanbieter eignen sich NTD-Verfahren. Zunächst einmal muss es einen „Gatekeeper“ geben, der einen Inhalt sperren kann und von dem man im Rahmen des Haftungsregimes auch vernünftigerweise erwarten kann, auf bestimmte Inhalte als Folge einer „Verdachtsmeldung“ im Einzelfall Einfluss zu nehmen. Die wichtigsten Anwendungsgebiete liegen daher v.a. beim Hosting, v.a. heutigen UGC-Plattformen mit ihren massenhaften nutzergenerierten Inhalten (YouTube, eBay, Facebook, usw.). In diesem Bereich liegt auch der Schwerpunkt der weltweit relevantesten gesetzlichen NTD-Regelung in § 512 U.S. Copyright Act (die aber auch für das Linking gilt).

Gesetzliche *notice and take-down* Verfahren (NTD) sind Teil gesetzlicher spezieller Haftungsprivilegierungen für Internetprovider. Als Teil dieser Haftungsprivilegierungen determiniert NTD *nicht* abschließend die