

Prüfungspflichten bei Rapidshare

Das Hanseatische Oberlandesgericht hat mit Urteil vom 02.07.2008 (Az. 308 O 19/07) erhöhte Prüfungspflichten für rapidshare angenommen. Die vom BGH entwickelte Begrenzungen von Prüfungspflichten für Dienstbetreiber könne bei Anbietern wie rapidshare nicht gelten, weil solche Geschäftsmodelle Urheberrechtsverletzungen Vorschub leisten würden und durch das Ermöglichen anonymer Uploads dem Berechtigten jede Verfolgungsmöglichkeit genommen werde.

Auch zur Frage, ob Rapidshare IP-Adressen gespeichert hat und wie der Shared-Hoster damit umgegangen ist kann das Urteil Klarheit verschaffen:

Der Dienst werde jedermann zur Verfügung gestellt, wobei grundsätzlich Anonymität gewährleistet sei. Auf die Erhebung personenbezogener Daten habe Rapidshare insoweit bewusst verzichtet. Eine Anmeldung oder Identitätskontrolle finde daher nicht statt.

Beim Hochladen (Upload) von Dateien werde jedoch die IP-Adresse des Absenders festgehalten. Eine Rückverfolgung von Dateien, aus dem außereuropäischen Ausland sei ? auch in Abhängigkeit von der in dem jeweiligen Land bestehenden Gesetzeslage ? zum Teil nur eingeschränkt möglich. Das Herunterladen der Dateien stehe jeder Person anonym zur Verfügung. Die Nutzungsmöglichkeit bestehe zum Teil kostenfrei, im Rahmen eines "Premium Account" gebührenpflichtig bei verbessertem Service, allerdings bei eingeschränkter Anonymität. Ob Rapidshare IP Adressen auch beim Download speichert, bleibt offen. Rapidshare habe allerdings in der Vergangenheit die Herausgabe dieser Daten regelmäßig verweigert.

amtliche Leitsätze:

1. Ein Geschäftsmodell, das aufgrund seiner Struktur durch die Möglichkeit des anonymen Hochladens in Pakete zerlegter, gepackter und mit Kennwort gegen den Zugriff geschützter Dateien der massenhaften Begehung von Urheberrechtsverletzungen wesentlich Vorschub leistet, kann von der Rechtsordnung nicht gebilligt werden. Die von dem Bundesgerichtshof zum Schutze des Dienstbetreibers vorgesehenen Begrenzungen von Prüfungspflichten können insbesondere dann nicht Platz greifen, wenn der Betreiber ihm zumutbare und nahe liegende Möglichkeiten, die Identität des Nutzers zum Nachweis einer etwaigen Wiederholungshandlung festzustellen, willentlich und systematisch ungenutzt lässt.

2. Lässt der Betreiber eines Sharehosting-Dienstes in Kenntnis begangener Urheberrechtsverletzungen weiterhin einschränkungslos eine anonyme Nutzung seines

Dienstes zu, schneidet er dem verletzten Urheber sehenden Auges den erforderlichen Nachweis wiederholter Begehungshandlungen ab, welchen dieser benötigt, um auf der Grundlage der höchstrichterlichen Rechtsprechung seine Rechte erfolgreich und wirksam durchsetzen können. In diesem Fall kann sich der Betreiber zur Vermeidung seiner Verantwortlichkeit als Störer unter bestimmten Voraussetzungen nicht mehr auf eine ansonsten gegebenenfalls bestehende Unzumutbarkeit umfangreicher Prüfungspflichten berufen.

Hanseatisches Oberlandesgericht, Urteil vom 02. Juli 2008, 5 U 73/07 (rechtskräftig)

In dem Rechtsstreit

...

hat das Hanseatische Oberlandesgericht Hamburg, 5. Zivilsenat, durch die Richter Betz, Rieger, Dr. Koch nach der am 9. April 2008 geschlossenen mündlichen Verhandlung für Recht erkannt:

Auf die Berufung der Antragsgegner wird das Urteil des Landgerichts Hamburg, Zivilkammer 8, vom 09. März 2007 teilweise ? insoweit unter Aufhebung der einstweiligen Verfügung vom 11. Januar 2007 und Zurückweisung des auf ihren Erlass gerichteten Antrags ? abgeändert und der Tenor der einstweiligen Verfügung vom 11. Januar 2007 wie folgt neu gefasst:

Die Antragsgegner werden verurteilt, es bei Meidung eines vom Gericht für jeden Fall der Zuwiderhandlung festzusetzenden Ordnungsgeldes bis zu EUR 250.000.-, ersatzweise Ordnungshaft oder Ordnungshaft bis zu 6 Monaten, zu unterlassen,

im Rahmen des Online-Dienstes www...com

die Computerprogramme "IBM Lotus Organizer" gemäß Anlage I zur einstweiligen Verfügung vom 11.01.07 oder "IBM Total Storage Productivity Center V 3.2.1 Agent, AIX, Multilingual" gem. Anlage II zu der genannten einstweiligen Verfügung

zu vervielfältigen oder öffentlich zugänglich zu machen und/oder vervielfältigen oder öffentlich zugänglich machen zu lassen.

Die weitergehende Berufung der Antragsgegner wird zurückgewiesen.

Von den Kosten des Rechtsstreits in erster und zweiter Instanz tragen die Antragsgegner wie Gesamtschuldner 80%, die Antragstellerin trägt 20%.

Gründe

I.

Die Antragstellerin ist Herstellerin von Hard- und Softwareprodukten für den privaten und gewerblichen Anwendungsbereich, die sie weltweit vertreibt.

Zu ihrer Produktpalette gehört unter anderem die Software IBM Lotus Organizer (Anlage AS 1 bis AS 3 sowie Anlage I). Hierbei handelt es sich um ein Computerprogramm zur Terminplanung. Weiterhin gehört zur Produktpalette der Antragstellerin die Softwarefamilie "IBM TotalStorage Productivity Center", die ein Teil des Softwarepakets "Tivoli" ist. Sie erlaubt es, verteilte Speicher-Infrastrukturen aufzubauen, zu verwalten und darauf zuzugreifen. Die Software "IBM Total Storage Productivity Center V 3.2.1 Agent, AIX, Multilingual" ist ein selbstständiger Teil dieser Softwarefamilie. Es handelt sich hierbei um eine komplexe Software für den geschäftlichen Anwendungsbereich, die über Vertragshändler vertrieben wird (Anlagen AS 5 bis AS 9).

Die Antragstellerin ist Inhaberin der Gemeinschaftsmarke Nr. 900316 "Lotus", die unter anderem in Klasse 9 für Computerprogramme geschützt ist; weiterhin ist die Antragstellerin Inhaberin der Gemeinschaftsmarke Nr. ... "IBM" sowie der Gemeinschaftsmarke Nr. ... "Totalstorage" (Anlage AS 10).

Die Antragsgegner betreiben unter der Bezeichnung "Rapidshare" einen sog. Sharehosting-Service. Sie stellen dabei dritten Personen Serverplatz zur Hinterlegung von Dateien zur Verfügung, die diese Nutzer auf ihre Server vollautomatisch hochladen können. Diese Daten können anschließend von anderen Internet-Nutzern zur Nutzung heruntergeladen werden (Anlage AS 11). Die Grundkonzeption des Dienstes "Rapidshare" war nach Darstellung der Antragsgegner diejenige eines reinen Hosting-Dienstes, durch welchen lediglich Webespace zur Verfügung gestellt werden sollte. Gedacht war insbesondere an nicht versierte Internet-Nutzer, die mittelgroße (2 bis 100 MB), private Datenmengen wie Lichtbilder bzw. Videos, die sich wegen ihres Volumens für den Versand per E-Mail nicht eigneten, Freunden und Bekannten zugänglich machen wollten. Für diese Nutzergruppe sollte das Hochladen von Dateien so unkompliziert wie möglich gestaltet werden. Die hochgeladenen Dateien sollten ausschließlich für den jeweiligen Nutzer gespeichert werden,

nicht jedoch einer unbeschränkten Zahl von Personen zur Verfügung gestellt oder über Suchfunktionen allgemein verfügbar gemacht werden. Es war beabsichtigt, den Schutz persönlicher Daten zu gewährleisten (vgl. Anlage BK 20). Den berechtigten Nutzern der Dateien muss deshalb von derjenigen Person, die die Dateien hoch geladen hat, die konkrete Speicheradresse mitgeteilt werden, die der Veranlasser beim Einstellen in den Dienst ? ebenso wie die Adresse zum Löschen der Datei ? als Link (z. B. in der Struktur wie <http://...com/files/22561795/Test.pdf.html>, vgl. Anlage BK 18 für den Dienst Rapidshare.com) zur Verfügung gestellt bekommt. Andernfalls können die Dateien nicht gezielt gefunden werden. Der Dienst der Antragsgegner war nach ihren Angaben ? anders als z. B. sog. Filesharing-Dienste ? für eine Verbreitung von Dateien an eine breite Öffentlichkeit ursprünglich nicht vorgesehen.

Der Antragsgegner zu 2. betreibt unter der Einzelfirma RapidTec den Dienst "rapidshare.de". Die Antragsgegnerin zu 1. ist Betreiberin des Dienstes "rapidshare.com" (Anlage AS 12). Der Antragsgegner zu 2. ist Inhaber der Domainnamen "rapidshare.de" und "rapidshare.com" (Anlage AS 13). Der Antragsgegner zu 2. ist zudem gemeinsam mit einem Herrn B.C. Verwaltungsrat der in der Schweiz ansässigen Antragsgegnerin zu 1. (Anlage AS 14 und AS 58).

Der Dienst wird jedermann zur Verfügung gestellt, wobei grundsätzlich Anonymität gewährleistet ist. Auf die Erhebung personenbezogener Daten haben die Antragsgegner bewusst verzichtet. Eine Anmeldung oder Identitätskontrolle findet nicht statt. Bei dem Hochladen von Dateien wird nur die IP-Adresse des absendenden Servers festgehalten. Eine Rückverfolgung von Dateien, die von Servern hoch geladen werden, die im außereuropäischen Ausland stehen, ist ? auch in Abhängigkeit von der in dem jeweiligen Land bestehenden Gesetzeslage ? zum Teil nur eingeschränkt möglich. Das Herunterladen der Dateien steht ebenfalls jeder Person anonym zur Verfügung. Die Nutzungsmöglichkeit besteht zum Teil kostenfrei, im Rahmen eines "Premium Account" gebührenpflichtig bei verbessertem Service, **allerdings bei eingeschränkter Anonymität** (Anlage AS 18).

Das Nutzungskonzept der Antragsgegner ist zwar auf die Einstellung größerer legaler Datenmengen ausgerichtet. Im Hinblick auf die Anonymität und die große Speicher- und Übertragungskapazität der von den Antragsgegnern bereitgestellten Dienste sind diese allerdings auch für den Austausch von Raubkopien attraktiv und in der einschlägigen Szene bekannt (Anlage AS 20), ohne dass die Antragsgegner ? nach ihrer eigenen Darstellung ? diese Art der Nutzung wünschen. Für das Herunterladen illegaler Kopien urheberrechtlich geschützter Software werden die Download-Adressen bei den Diensten der Antragsgegner auf bestimmten, "einschlägigen" Internetseiten ("Raubkopiererseiten") interessierten

Nutzern mitgeteilt, so dass diese sich mit den dort veröffentlichten Links unmittelbar die Raubkopien von dem Dienst der Antragsgegner verfügbar machen können.

Unter der Rubrik "Häufig gestellte Fragen" (FAQ) findet sich auf beiden Internetseiten u. a. folgender Hinweis (Anlage AS 22):

- Welche UPLOAD-REGELN sind zu befolgen?
- Keine Dateien, die nicht zum Verteilen freigegeben sind (verbotene, pornografische oder geschützte Werke)"

Im Impressum beider Internetseiten heißt es:

"illegale Dateien werden sofort nach Kenntnisnahme entfernt und auf unseren Dateifilter gesetzt. Bitte schreiben Sie eine Mail mit den genauen Dateilinks an unsere Abuse-Abteilung."

Die Antragsgegner setzen unter anderem einen sog. MD5-Filter ein, der verhindert, dass inhaltlich identische Dateien erneut hoch geladen werden können. Weiterhin überprüfen sie automatisiert die Namen hoch geladener Dateien darauf, ob sich in den Dateien Namen bestimmte Worte (z. B. "IBM") bzw. Wortkombinationen (z. B. "Total" und "Storage") finden, die auf eine Rechtsverletzung hindeuten.

Von Raubkopierern werden z. B. gepackte Dateien unter Verwendung eines Verschlüsselungsalgorithmus auf die Dienste der Antragsgegner hochgeladen, sodass ein Entpacken ? und damit eine Überprüfung der Dateien durch die Antragsgegner auf etwaige Rechtsverletzungen ? ohne Kenntnis des Verschlüsselungscodes nicht möglich ist.

Der Mitarbeiter D.O. der Abuse-Abteilung der Antragsgegner hatte auf eine Nutzeranfrage u. a. folgende Auskunft gegeben, die in einem Forum verfügbar (gemacht worden) war (Anlage AS 23):

"We are bound to delete all files which are reported to us. Sorry, but we can't control each individual file, if it is still legal. If your file really is legal, you can upload it again, you only have to C.e one ore more bits of the file. You can pack it for example."

Auch in einschlägigen Nutzerforen finden sich zum Teil Hinweise darauf, wie Schutzmaßnahmen von "Rapidshare" umgangen werden können (Anlage AS 30 und 31) bzw. wie der Dienst der Antragsgegnerin in einer Weise genutzt wird, dass sich die mit dem

Premium Account verbundenen Gebühren rentieren (Anlage AS 31a).

Im Oktober 2006 leitete der Antragsgegner zu 2. den kostenlosen Sharehosting-Service als Massengeschäft für künftige Nutzungen unter Hinweis darauf, dass alle Festplattenkapazitäten ausgeschöpft seien, von "rapidshare.de" auf "rapidshare.com" über (Anlagen AS 34 bis AS 38). Der Dienst über die Internetseite "rapidshare.de" blieb zunächst als exklusiver Hosting-Dienst für zahlende Premium-Kunden aufrechterhalten, deren Identität der Antragsgegner zu 2. über entsprechende Finanzdienstleister feststellen konnte. Über den Dienst unter der Domainadresse rapidshare.com sollte zukünftig in erster Linie das kostenlose "Massengeschäft" abgewickelt werden. Dieser Dienst ist u. a. stärker international ausgerichtet und verfügt dementsprechend auch über eine nicht unerhebliche Zahl ausländischer Nutzer. Im Übrigen ist der Dienst rapidshare.com strukturell mit dem Dienst rapidshare.de vergleichbar. Insbesondere wird in beiden Fällen Dritten die Möglichkeit zur Speicherung von Daten zur Verfügung gestellt, ohne dass der jeweilige Betreiber des Dienstes von deren Inhalt Kenntnis hat oder über die konkrete Art der Weitergabe der Daten an Dritte (mit)entscheidet. Über den Dienst rapidshare.com werden gegenwärtig täglich ca. 150.000 neue Dateien hoch geladen, was einem Dateivolumen von über 6 Terrabyte entspricht. Die Antragsgegner haben in der Senatsverhandlung unstreitig gestellt, dass auch der Dienst www...de seit einiger Zeit wieder ohne Registrierung anonym genutzt werden kann.

Die Antragstellerin stellte ebenfalls im Oktober 2006 fest, dass Raubkopien einer Vielzahl ihrer Softwareprodukte, unter anderem der im Verfügungsantrag genannten Produkte, über den Dienst Rapidshare von nicht näher identifizierbaren Nutzern (Anlage AS 40) zum Download bereitgestellt wurden (Anlage AS 39). Von welchen Personen die beanstandeten Raubkopien der Dateien der Antragstellerin auf den Server der Antragsgegner hoch geladen worden sind, hat sich auch später nicht feststellen lassen. Der Datei-Upload ist durch Provider mit Sitz in M. bzw. T. erfolgt (Anlage AS 46). Anfragen sind insoweit unbeantwortet geblieben. Die Antragsgegner haben sich geweigert, die insoweit zugeordneten IP-Adressen zu sperren.

Die Antragstellerin forderte die Antragsgegner mit E-Mail vom 13.10.06 zur sofortigen Löschung der auf Raubkopien verweisenden Links auf. Sie erhielt mit E-Mail vom 17.10.06 von dem Mitarbeiter D. O. der Antragsgegner eine Bestätigung, dass die beanstandeten Dateien vom Server gelöscht und auf eine schwarze Liste gesetzt worden seien (Anlage AS 41).

Mit Schreiben ihrer Prozessbevollmächtigten vom 13.10.06 mahnte die Antragstellerin sodann den Antragsgegner zu 2. ab und forderte diesen zur Abgabe einer

Unterlassungserklärung auf (Anlage AS 42). Mit Schriftsatz seiner Prozessbevollmächtigten vom 16.10.06 (Anlage AS 43) gab der Antragsgegner zu 2. daraufhin eine strafbewehrte Unterlassungserklärung ab, die sich indes zunächst entgegen dem Verlangen der Antragstellerin nicht auf die zur Nutzung bereitgehaltenen Programme, sondern lediglich auf bestimmte, in der Vergangenheit genutzte Speicheradressen bezog. Nach weiterem rechtsanwaltlichen Schriftwechsel gab der Antragsgegner am 23.10.06 eine entsprechend erweiterte Unterwerfungserklärung ab (Anlage AS 44 bis 45). Ein weiterer Schriftwechsel sowie telefonischer Kontakt der Partei-Vertreter schloss sich an (Anlagen AS 59 bis AS 61).

Im Anschluss an einen erneuten Verletzungsfall, den die Antragstellerin im November 2006 entdeckt hatte (Anlage AS 47), mahnte die Antragstellerin den Antragsgegner mit E-Mail ihrer Prozessbevollmächtigten vom 22.11.06 erneut ab (Anlage AS 48).

Daraufhin gab die Antragsgegnerin zu 1. mit Schreiben ihrer Prozessbevollmächtigten vom 30.11.06 eine weitere Unterlassungserklärung ab, die sich auf die von der Antragstellerin beanstandeten Links, nicht jedoch auf eine allgemeine Unterwerfung im Hinblick auf die hierüber zu beziehende Software bezog (Anlage AS 49). Diese beanstandete die Antragstellerin als unzureichend (Anlage AS 50). Die Abgabe einer weitergehenden Unterwerfungserklärung lehnte die Antragsgegnerin zu 1. mit Schreiben ihrer Prozessbevollmächtigten vom 15.12.06 ab (Anlage AS 51). In der Folgezeit kam es zu weiteren Uploads von Raubkopien urheberrechtlich geschützter Produkte der Antragstellerin über den Dienst www...com (Anlage AS 52 bis AS 57).

Die Antragstellerin hat daraufhin am 09.01.07 bei dem Landgericht Hamburg einen Antrag auf Erlass einer einstweiligen Verfügung gestellt. Sie macht sowohl urheberrechtliche als auch markenrechtliche Unterlassungsansprüche geltend und hat vorgetragen,

unter den Domains www...de und www...com der Antragsgegner würden ständig Raubkopien ihrer Softwareprodukte zum Download durch Dritte bereitgestellt. Die Website sei allgemein als Umschlagplatz für Raubkopien bekannt (Anlage AS 20, Anlage AS 32, Anlage AS 33). Mit ihrem Geschäftsmodell wendeten sich die Antragsgegner gezielt an Raubkopierer, die für ihr verbotenes Tun dank der Anonymität keine Konsequenzen zu fürchten hätten.

Die Antragsgegner vermieden es, ihre Nutzer vom Upload von Raubkopien abzuschrecken. Die von ihnen gegebenen, versteckten Hinweise seien unzureichend. Für den Nutzer sei insbesondere ersichtlich, dass ernsthafte Konsequenzen im Fall des Einstellens von Raubkopien nicht drohten. Im Gegenteil ? der Mitarbeiter D. O. der Antragsgegner habe durch seinen als Anlage AS 23 vorgelegten Foren-Beitrag sogar unverhohlenen Hinweise

gegeben, wie einfach die Sperrung als illegal erkannter Dateien jederzeit umgangen werden könnte, nämlich durch die Veränderung einzelner Bits oder durch das Packen der Dateien. Hierdurch werde letztlich zum Rechtsmissbrauch aufgefordert.

Die Antragsgegner seien als Störer bzw. Teilnehmer für die Urheberrechtsverletzungen der Nutzer ihres Dienstes verantwortlich. Sie verzichteten pflichtwidrig auf jede Art der Nutzerkontrolle bzw. Pflicht zur Identifizierung. Es bestünden weder rechtsverbindliche Verpflichtungen der Nutzer noch Sanktionen im Fall von rechtswidrigen Nutzungen, wie dies bei anderen Diensten üblich sei (Anlage AS 21 für X). Dadurch vereitelten die Antragsgegner die Durchsetzung von Schutzrechten. Dies auch dadurch, indem sie auf Online-Suchfunktionen, Inhaltsverzeichnisse oder sonstige Suchinstrumente verzichteten. Das Auffinden und Herunterladen der Raubkopien setzte die Kenntnis eines Links zum entsprechenden Speicherort auf den Servern der Antragsgegner voraus und, sofern die Dateien vom Absender entsprechend verschlüsselt worden seien, auch die Kenntnis des beim Upload vergebenen Passworts. Auf diese Weise sei es möglich, dass die entsprechenden Hinweise auf Links in der einschlägigen Szene weitergegeben werden könnten, ohne dass Rechteinhaber davon Kenntnis erhielten.

Der von den Antragsgegnern eingesetzte Dateifilter nach dem MD5-Verfahren (Anlage AS 24) sei letztlich wirkungslos. Es sei auch möglich, entdeckte und gelöschte Raubkopien jederzeit wieder hochzuladen. Bereits bei dem erneuten Packen einer Datei (ohne inhaltliche Veränderung) mit einem üblichen Komprimierungsprogramm ? Verwendung finde häufig das bei Raubkopien gängige *.rar-Format (Anlage AS 27 bis AS 29) ? ändere sich die Prüfsumme (Anlage AS 26), sodass diese von dem MD5-Verfahren nicht mehr erkannt würde. Um das erneute Hochladen illegaler Software zu erkennen, müssten deshalb die zu Archiven gepackten Dateien von den Antragsgegnern entpackt werden, um die Prüfsummen der darin enthaltenen Einzeldateien darauf zu überprüfen, ob es sich hierbei um bereits bekannte und gesperrte Software handele. Eine solche Prüfung nähmen die Antragsgegner aber nicht vor. Auch eine inhaltliche Prüfung der Dateien, durch die die Identität von Raubkopien aufgespürt werden könnte, finde bei den Antragsgegnern gerade nicht statt.

Es wäre den Antragsgegnern ohne weiteres möglich gewesen, diesen Missbrauch durch den Einsatz ihnen zumutbarer Filtersoftware bzw. sonstiger Prüfprogramme zu entdecken und zu unterbinden. Derartige Methoden seien verfügbar. Insoweit wird auf die Ausführungen der Antragstellerin auf Seiten 14/15 der Antragschrift Bezug genommen. Die Antragsgegner hätten sich zu Unrecht geweigert, derartige Programme zu verwenden.

Das Geschäftsmodell der Antragsgegner sei nach den Grundsätzen der

BGH-Rechtsprechung nicht schutzwürdig, weil es auf nachhaltige und systematische Rechtsverletzungen angelegt sei.

Die Antragstellerin hat in erster Instanz beantragt,

die Antragsgegner zu verurteilen, es bei Meidung eines vom Gericht für jeden Fall der Zuwiderhandlung festzusetzenden Ordnungsgeldes bis zu EUR 250.000.-, ersatzweise Ordnungshaft oder Ordnungshaft bis zu 6 Monaten, zu unterlassen,

die Computerprogramme "IBM Lotus Organizer" gemäß Anlage I zum Antrag oder "IBM Total Storage Productivity Center V 3.2.1 Agent, AIX, Multilingual" gem. Anlage II zum Antrag

zu vervielfältigen oder öffentlich zugänglich zu machen oder vervielfältigen oder öffentlich zugänglich machen zu lassen

und/oder

Computerprogramme unter der Bezeichnung "IBM" und/oder "Lotus Organizer" und/oder "Total Storage Productivity Center V 3.2.1 Agent, AIX, Multilingual" anzubieten oder zu vertreiben oder anbieten oder vertreiben zu lassen.

Auf der Grundlage dieses Antrags hat das Landgericht Hamburg mit Beschluss vom 11.01.07 eine einstweilige Verfügung gegen die Antragsgegner erlassen, der als Anlagen I + II zwei CD-ROMs mit den betreffenden Programmen beigelegt sind. Hiergegen richtet sich der Widerspruch der Antragsgegner, mit dem diese in erster Instanz begehrt haben, die einstweilige Verfügung aufzuheben und den Verfügungsantrag zurückzuweisen.

Die Antragsgegner machen geltend,

sie kämen den ihnen obliegenden Prüfungs- und Sorgfaltspflichten in vollem Umfang nach und gingen sogar noch über ihre rechtlichen Pflichten hinaus. Eine Verantwortlichkeit als Störer bzw. Täter einer Urheberrechtsverletzung sei deshalb ausgeschlossen.

Der Anteil von Raubkopien auf ihren Servern bewege sich im niedrigen einstelligen Prozent-Bereich. Der von der Antragstellerin vermittelte Eindruck, ihre Dienste würden im Wesentlichen durch den Austausch illegaler Ware geprägt, sei offensichtlich falsch. Sie selbst missbilligten nachdrücklich den Missbrauch ihre Dienste durch Raubkopierer. Sie

seien bestrebt, einen derartigen Missbrauch nach Kräften zu verhindern. Dabei seien die von ihnen ergriffenen Maßnahmen bereits weit über das rechtlich geschuldete Maß hinaus gegangen. Dies schließe zwar nicht aus, dass es Raubkopierern nach wie vor gelinge, neue Raubkopien hoch zu laden bzw. alte Raubkopien so zu verändern, dass sie nicht mehr von den Schutzmaßnahmen herausgefiltert würden. Weitergehende Kontrollsysteme seien ihnen jedoch nicht zumutbar. Bereits die gegenwärtigen Überprüfungsmaßnahmen erforderten ein sehr hohes Maß an Aufwand durch ihre Abuse-Abteilung. Allein die Antragsgegnerin zu 1. beschäftige sechs Mitarbeiter in ihrer Abuse-Abteilung, die Einstellung weiterer vier Mitarbeiter für diese Abteilung sei geplant.

Sie, die Antragsgegner, stellten einigen größeren Rechteinhabern zudem einen Zugang zur Verfügung, mit dem diese innerhalb kürzester Zeit unmittelbar selbst rechtswidrige Dateien aus dem Angebot der Antragsgegner löschen könnten, sofern sie diese vor den Mitarbeitern der Abuse-Abteilung entdeckten. Diese Möglichkeit bestehe auch für die Antragstellerin (Anlage AG 4). Sie hätten zudem ihre Bereitschaft bekundet, mit den Technikern und Programmierern der Antragstellerin Kontakt aufzunehmen, um gemeinsam daran zu arbeiten, den Software-Filter ihrer Dienste weiter zu verbessern. Die Antragstellerin habe von allen diesen Angeboten keinen Gebrauch gemacht.

Es sei für sie im Übrigen auch überhaupt nicht feststellbar, ob es sich bei den hoch geladenen Dateien um Raubkopien handle. Denn gem. § 69c Nr. 1 UrhG sei auch jeder berechnigte Nutzer ohne Zustimmungsvorbehalt berechnigt, eine (Sicherungs)Kopie herzustellen. Es sei ihnen nicht möglich zu überprüfen, ob es sich bei den hoch geladenen Dateien um derartige zulässige Vervielfältigungen handle.

Die Dienste "rapidshare.de" und "rapidshare.com" basierten zwar auf derselben Geschäftsidee, seien indes ansonsten nicht identisch, sondern zeigten erhebliche Unterschiede.

Der konsequente Verzicht ihrer Dienste darauf, Suchfunktionen oder Dateilisten zur Verfügung zustellen, sei allein durch das Bestreben veranlasst, die Privatsphäre bzw. das Berufs- oder Geschäftsgeheimnis ihrer Nutzer schützen zu können.

Es sei gegenwärtig technisch unmöglich, eine Software zu entwickeln, die jeder beliebigen Datei ansehen könne, ob sie eine Raubkopie sei oder nicht. Er, der Antragsgegner zu 2., habe daraufhin den "MD5-Filter" entwickelt, um das erneute Upload bekannter und bereits gelöschter illegaler Dateien zu verhindern. Die von ihnen derzeit eingesetzten Filterverfahren seien ausgesprochen effektiv. Darüber hinaus habe er ein Programm entwickelt, welches die Dateinamen überprüfe und bei dem Auftauchen verdächtiger

Dateinamen unverzüglich interne Kontrollmaßnahmen durch die Abuse-Abteilung einleite. Es seien bereits vor der Beanstandung durch die Antragstellerin 1.039 Dateien gelöscht worden, die einen verdächtigen, auf die Antragstellerin hinweisenden Zusatz im Dateinamen gehabt hätten (Anlage AS 13) Zudem überprüften sie stichprobenartig immerhin 604 einschlägig bekannte Internetseiten nach Hinweisen auf offensichtliche Rechtsverletzungen über ihre Dienste (Anlage AG 12).

Zu ihren Gunsten gelte die Haftungsprivilegierung des §§ 10 Satz 1 TMG. Die gegenteilige Rechtsprechung des Bundesgerichtshofs sei nicht überzeugend. Die Behauptung der Antragstellerin, sie hätten über ihren Mitarbeiter in Nutzerforen selbst Hinweise dazugegeben, wie Schutzmechanismen zu überwinden seien, sei unzutreffend. Die entsprechende Antwort aus einer individuellen Kommunikation sei in das Forum einkopiert worden. Dabei sei ihr Mitarbeiter D. O. offenbar selbst Opfer von Raubkopierern geworden, die sich als unauffällige Nutzer ausgegeben, tatsächlich aber versucht hätten, Umgehungsmöglichkeiten des Filters in Erfahrung zu bringen. Ohnehin ergebe sich aus dem Internetforum, dass sich eine Vielzahl von Nutzern darüber beschwerten, dass die Antragsgegner zu viele ? auch legale ? Dateien auf Beanstandungen von Dritten bzw. wegen des Verdachts einer Rechtsverletzung löschten. Auch vor diesem Hintergrund sei der ihnen von der Antragstellerin gemachte Vorwurf unbegründet.

Er, der Antragsgegner zu 2., habe von den beanstandeten Rechtsverletzungen auch keine Kenntnis gehabt, sodass er schon deshalb nicht passiv legitimiert sei. Die allgemeine Kenntnis von der Gefahr eines derartigen Missbrauchs sei nicht ausreichend.

Markenrechtliche Ansprüche seien unbegründet, weil sich die Kennzeichen der Antragstellerin in gepackten und komprimierten sowie in zwei getrennten Dateien befunden hätten, so dass eine markenmäßige Benutzung schon deshalb ausgeschlossen gewesen sei.

Die Antragstellerin hat beantragt,

den Widerspruch abzuweisen und die einstweilige Verfügung zu bestätigen.

Sie trägt vor,

die Ausführungen der Antragsgegner seien zum Teil unzutreffend, zum Teil unerheblich. Letztlich weigerten sich die Antragsgegner, die ihnen obliegenden und zumutbaren Sicherungsmaßnahmen vorzunehmen. Es sei unzutreffend, dass das Entpacken einer Datei einen längeren Zeitraum in Anspruch nehme. Dies sei in wenigen Sekunden zu

bewerkstelligen und dauere nicht länger als das Kopieren einer Datei. Es biete auch keine Schwierigkeiten, in den entpackten Archiven gezielt nach ausführbaren Dateien und innerhalb dieser nach bestimmten Hinweisen auf Raubkopien zu suchen, ohne dass die Gefahr bestehe, zugleich unverdächtige Dateien zu sperren. Der Gefahr von Viren bzw. Archivbomben könnten die Antragsgegner durch entsprechende Schutzprogramme begegnen.

Tatsächlich nähmen die Antragsgegner die von ihnen behaupteten Überprüfungen noch nicht einmal vor. So sei es möglich gewesen, eine Datei, in deren Namen sich der Begriff "Lotus Organizer" befinde, selbst im Verlaufe des vorliegenden Verfahrens noch auf den Server hochzuladen, obwohl nach Darstellung der Antragsgegner insoweit Kontrollen stattfänden.

Für eine markenmäßige Benutzung reiche es bereits aus, dass die für sie geschützten Kennzeichen bei Kunden nach der Installation der Raubkopien sichtbar würden (Anlage AS 76).

Das Landgericht Hamburg hat mit dem angegriffenen Urteil vom 09. März 2007 die einstweilige Verfügung bestätigt und den hiergegen gerichteten Widerspruch zurückgewiesen. Hiergegen richtet sich die form- und fristgerecht eingelegte Berufung der Antragsgegner. Die Antragsgegner verfolgen in zweiter Instanz ihr Antragsabweisungsbegehren unter Vertiefung ihres erstinstanzlichen Sachvortrags weiter.

Die Antragsgegner beantragen nunmehr,

das Urteil des Landgerichts Hamburg vom 09.03.07 abzuändern und die einstweilige Verfügung unter Zurückweisung des auf ihren Erlass gerichteten Antrags aufzuheben.

Die Antragstellerin verteidigt das landgerichtliche Urteil auf der Grundlage der bereits erstinstanzlich gestellten Anträge, die sie in zweiter Instanz in folgender Form zur Entscheidung stellt,

die Berufung mit der Maßgabe zurückzuweisen, die Antragsgegner zu verurteilen, es bei Meidung eines vom Gericht für jeden Fall der Zuwiderhandlung festzusetzenden Ordnungsgeldes bis zu EUR 250.000.-, ersatzweise Ordnungshaft oder Ordnungshaft bis zu 6 Monaten, zu unterlassen,

1. die Computerprogramme "IBM Lotus Organizer" gemäß Anlage I zum Antrag oder "IBM Total Storage Productivity Center V 3.2.1 Agent, AIX, Multilingual" gem. Anlage II zum

Antrag

zu vervielfältigen oder öffentlich zugänglich zu machen oder vervielfältigen oder öffentlich zugänglich machen zu lassen

und/oder

2. im geschäftlichen Verkehr im Rahmen eines Online-Dienstes

Computerprogramme unter der Bezeichnung "IBM" und/oder "Lotus Organizer" und/oder "Total Storage Productivity Center V 3.2.1 Agent, AIX, Multilingual" anzubieten oder zu vertreiben oder anbieten oder vertreiben zu lassen.

Wegen der tatsächlichen Feststellungen im Übrigen wird auf den Tatbestand des landgerichtlichen Urteils sowie auf die von den Parteien zur Akte gereichten Schriftsätze nebst Anlagen Bezug genommen.

II.

Die zulässige Berufung ist überwiegend unbegründet. Der Antragstellerin steht der geltend gemachte urheberrechtliche Anspruch aus §§ 97 Abs. 1, 19a, 16 UrhG in dem aus dem Tenor ersichtlichen Umfang zu. Die Antragsgegner sind nach diesen Vorschriften zur Unterlassung verpflichtet. Eine markenrechtliche Unterlassungspflicht der Antragsgegner gem. § 14 Abs. 2, Abs. 5 MarkenG besteht hingegen nach Auffassung des Senats nicht.

1. Der Senat hat den Rechtsstreit als Berufungsgericht gemäß §§ 538 Abs. 1 ZPO selbst zu entscheiden. Eine Rückverweisung an das Landgericht kommt nicht in Betracht.

a. Soweit die Antragsgegner mit der Berufungsbegründung den Vorwurf erheben, das Landgericht habe mit dem angegriffenen Urteil gegen das in Art. 3 Abs. 1, 20 Abs. 3 GG niedergelegte Willkürverbot sowie gegen ihren Anspruch auf rechtliches Gehör gem. Art. 103 Abs. 1 GG verstoßen, das Urteil erschöpfe sich in leeren Phrasen und lasse jedwede Auseinandersetzung mit den streitentscheidenden Fragen vermissen, teilt der Senat diese Auffassung nicht. Das Landgericht hat sich mit den maßgeblichen tatsächlichen und rechtlichen Aspekten auseinander gesetzt, ist hierbei allerdings nicht zu dem von den Antragsgegnern gewünschten Ergebnis gelangt. Dies rechtfertigt jedoch nicht die von ihnen erhobenen Vorwürfe. Das Landgericht hat im Ausgangspunkt zutreffend festgestellt, dass die Antragsgegner Prüfungspflichten verletzt haben, weil sie keine ausreichenden Maßnahmen unternommen haben, um vorhersehbare Rechtsverletzungen in einem ihnen

zumutbaren Umfang nach Kräften zu vermeiden. Der Umfang sowie der Anlass derartiger Prüfungspflichten bedarf ? wie im Folgenden noch auszuführen sein wird ? noch erheblicher Konkretisierungen. Das Landgericht war entgegen der Auffassung der Antragsgegner allerdings nicht verpflichtet oder gehalten, diesen im Einzelnen zu erläutern, welche Art von Maßnahmen sie konkret zu ergreifen haben. Dies zu beurteilen, obliegt allein den Antragsgegnern. Das Landgericht konnte sich darauf beschränken festzustellen, dass die Antragsgegner ihnen zur Verfügung stehende und zumutbare Maßnahmen nicht ausgeschöpft haben. Bereits dies rechtfertigt dem Grunde nach ihre Verantwortlichkeit nach § 97 Abs. 1 UrhG.

b. Unabhängig davon zeigen die Antragsgegner auch keine rechtlichen Konsequenzen der von ihnen erhobenen Vorwürfe auf. Insbesondere sind die Voraussetzungen für eine Zurückverweisung an das Landgericht gem. § 538 Abs. 2 ZPO schon aufgrund ihrer eigenen Darlegungen nicht gegeben.

2. Die auch im Berufungsverfahren zu prüfende internationale Zuständigkeit des Senats im Verhältnis zu der Antragsgegnerin zu 1. ergibt sich aus Art. 5 Nr. 3 des EuGVVO (zur entsprechenden Rechtslage bei Art. 5 Nr. 3 EuGVÜ: BGH GRUR 05, 431 ? Hotel Maritim).

3. Der Antragstellerin steht der für die Verfolgung von Ansprüchen im einstweiligen Verfügungsverfahren erforderliche Verfügungsgrund zur Seite. Soweit sie ihre Ansprüche auf urheberrechtliche Normen stützt, ergeben sich die Voraussetzungen insoweit aus §§ 935, 940 ZPO. Denn in urheberrechtlichen Streitigkeiten besteht eine gesetzliche Vermutung nicht. Die Frage, ob die Regelung des § 12 Abs. 2 UWG auf markenrechtliche Ansprüche zu übertragen ist, bedarf im vorliegenden Rechtsstreit keiner Entscheidung. Die Antragsgegner haben die Frage des Verfügungsgrundes mit der Berufung nicht mehr aufgegriffen, sodass auch der Senat hierzu von näheren Ausführungen absehen kann. Ohnehin ergibt sich aus dem Parteivortrag, dass die Antragstellerin unter Berücksichtigung der Komplexität der Sach- und Rechtslage sowie der Beschaffung der erforderlichen Informationen und vorgerichtlichen Aufforderungen vor einer Erfolg versprechenden Einleitung eines gerichtlichen Verfahrens ihre Ansprüche mit dem erforderlichen Nachdruck verfolgt hat.

4. Das von der Antragstellerin mit dem Verfügungsantrag begehrte Verbot ist i. S. v. § 253 Abs. 2 Nr. 3 ZPO hinreichend bestimmt. Die Antragsgegner beanstanden zu Unrecht die Fassung des Unterlassungsantrags bzw. -tenors.

a. Die von der Antragstellerin begehrte Verpflichtung, ein rechtswidriges Verhalten zu unterlassen, bezieht sich bzw. beschränkt sich jedenfalls nach der Antragsfassung (zum

Streitgegenstand siehe sogleich) nicht auf einen bestimmten Dienst bzw. eine bestimmte Internet-Domain. Dementsprechend wären die Antragsgegner bei einer Berechtigung des geltend gemachten Anspruchs in diesem weiten Umfang auch dann zur Unterlassung verpflichtet, wenn gleichartige Verletzungshandlungen von den Antragsgegnern unter einer anderen Domain-Adresse ermöglicht werden. Darüber hinaus ist der Antrag auch nicht auf ein Handeln in elektronischen Medien beschränkt, sondern erfasst ebenfalls rechtsverletzende Handlungen der genannten Art in jeder anderen Form. Dies ist zumindest unter dem Gesichtspunkt einer etwaigen Unbestimmtheit des Antrags nicht zu beanstanden. Davon zu unterscheiden ist die Frage, ob ein derartiges Verhalten von der Antragstellerin zum Streitgegenstand erhoben worden ist bzw. ob der Antrag auch insoweit begründet ist. Hierauf wird noch einzugehen sein.

b. Auch die in dem Verfügungsantrag aufgeführten Begehungsformen einer Urheberrechtsverletzung sind aus Sicht des Senats jedenfalls in der Antragsfassung bedenkenfrei. Es ist ? auch dies wird im Folgenden noch näher ausgeführt werden ? bereits denkbar, dass die Antragsgegner tatsächlich Täter der ihnen vorgeworfenen Urheberrechtsverletzung sein können, etwa weil sie gegen das Gebot verstoßen haben, ihnen obliegende Verkehrspflichten zur Verhinderung von Urheberrechtsverletzungen zu erfüllen. Selbst wenn man die Antragsgegner (lediglich) als Störer einer von dritten Personen begangenen Urheberrechtsverletzung ansieht, bleibt es dabei, dass das "Vervielfältigen" bzw. "Öffentlich zugänglich machen" bzw. "Anbieten" auf und mit Hilfe desjenigen Internet-Dienstes geschieht, für welchen die Antragsgegner verantwortlich sind. Da eine Teilnehmerhaftung in derartigen Fällen wegen des fehlenden (doppelten) Vorsatzes in der Regel ausscheidet, kommt eine abweichende Fassung der Unterlassungsanträge aus Sicht des Senats nicht in Betracht, wenn alle denkbaren Verletzungsformen erfasst werden sollen. Eine hiervon zu unterscheidende Frage ist, ob sie in dieser Weise auch nebeneinander materiell begründet sind.

5. Streitgegenstand nach dem ersten Teil des Verfügungsantrags ist ein urheberrechtlicher Verstoß. Der zweite Teil des Verfügungsantrages umschreibt einen davon zu unterscheidenden markenrechtlichen Verstoß. Streitgegenstand ist dabei nach dem gestellten Antrag zu 1. ein rechtsverletzendes Verhalten beider Antragsgegner unabhängig von dem verwendeten Medium. Nachhaltig streitig ist zwischen den Parteien, ob sich der Antrag und das Urteil des Landgerichts ausschließlich auf den Dienst www...com (für den beide Antragsgegner verantwortlich sind) oder auch auf den Dienst www...de (für den nur der Antragsgegner zu 2. zuständig ist) bezieht. Nach Auffassung des Senats ist der zuletzt genannte Dienst nicht Gegenstand des vorliegenden Rechtsstreits.

a. Die Antragstellerin steht auf den Standpunkt, beide Dienste seien von dem Verbot

umfasst. Diese Frage ist zwischen den Parteien streitig insbesondere im Zusammenhang mit den gestellten Ordnungsmittelanträgen 5 W 89/07 und 5 W 140/07 sowie mit den Parallelverfahren 5 U 119/07 und 5 U 149/07. Dementsprechend kann diese Frage auch nur im Rahmen einer Gesamtbetrachtung geklärt werden. Die Tatsache, dass die Antragsgegner ihren Dienst "rapidshare.com" gegründet haben, nachdem der Dienst "rapidshare.de" unter anderem wegen der Verbreitung urheberrechtswidriger Raubkopien in die Kritik geraten ist, verdeutlicht, dass aus Sicht der Antragstellerin auch eine konkrete Gefahr besteht, dass die Antragsgegner auf einen neuen Dienste ausweichen, wenn ihnen ein bestimmtes Verhalten unter ihren bisherigen Domain-Adressen verboten wird. Deshalb bestünde ? sofern man die anhängigen Parallelrechtsstreitigkeiten 5 U 119/07 und 5 U 149/07 zunächst nicht in die Betrachtung mit einbezieht ? grundsätzlich ein Rechtsschutzbedürfnis der Antragstellerin an einem derart umfassend formulierten Verbot. Denn vor dem Hintergrund des Verhaltens der Antragsgegner wäre nur ein solches Verbot, welches ein bestimmtes Verhalten ohne Rücksicht auf die Angebotsplattform untersagt, geeignet, den berechtigten Interessen der Antragstellerin Genüge zu tun.

b. Fraglich ist indes, ob sich der Verfügungsantrag auch hierauf erstreckt. Insoweit bedarf es der Auslegung des Verfügungsantrags auf der Grundlage der ihm beigelegten Begründung. Eine Sachentscheidung ? und ebenfalls der ihr zugrunde liegende Antrag ? kann unter Umständen lediglich unter Heranziehung des Parteivorbringens und der Urteilsgründe (vgl. BGH WRP 92, 560 ? Unbestimmter Unterlassungsantrag II) Aufschluss darüber geben, wie das konkret beanstandete Verhalten zu beurteilen ist (BGH WRP 00, 746, 748 ? Marlene Dietrich).

c. Das Landgericht hat insoweit keine Einschränkung auf einen bestimmten Dienst vorgenommen. Es hat sich allerdings in seinem Beschluss vom 22.06.07 in dem Ordnungsmittelverfahren 5 W 140/07 auf den Standpunkt gestellt, die Entscheidung erfasse beide Dienste www...de und www...com. Diese Auffassung vermag der Senat nicht zu teilen.

aa. Ausdrücklicher Gegenstand des Angriffs war ein Handeln unter dem Dienst www...de nicht. Die Antragsgegner weisen in dem Ordnungsmittelverfahren zutreffend daraufhin, dass bei ? zulässigerweise ? nicht begründeten gerichtlichen Entscheidungen zur Bestimmung der Reichweite des Verbots im Zweifelsfall auf das Parteivorbringen zurückzugreifen ist. Die Antragsgegner haben nochmals ausführlich dargelegt, dass sich sämtliche Ausführungen der Antragstellerin ausschließlich auf den Dienst www...com bezogen haben. Die Antragstellerin hatte das Handeln des Antragsgegners zu 2. unter seinem Dienst www...de (sowie Fragen der Domaininhaberschaft) in der Antragschrift zwar erwähnt, ohne aber das konkret beanstandete Handeln hierauf zu beziehen. Insbesondere

betrafen die im vorliegenden Verfahren erörterten Verletzungsfälle ausschließlich solche unter www...com.

bb. Auch eine Interpretation der Entscheidungsgründe des Landgerichts (dort Seite 13/14) ergibt, dass sich die Verurteilung nicht auf den Dienst www...de bezieht. Denn das Landgericht hat die Verantwortlichkeit des Antragsgegners zu 2. ausschließlich aus einer Funktion als Verwaltungsrat der Antragsgegnerin zu 1. abgeleitet. Der Senat entnimmt den Urteilsgründen damit, dass diese sich nur mit dem Dienst www...com beschäftigen, so dass davon auszugehen ist, dass sich die Entscheidung unausgesprochen auch nur hierauf bezieht. Zwar mag es sein, dass die konkrete Internet-Adresse nicht zum Kern der Verletzungshandlung gehört. Gleichwohl ist es auch vor dem Hintergrund des Bestimmtheitsgrundsatzes erforderlich, diese jedenfalls dann konkret anzugeben, wenn die in Anspruch genommenen Personen ? wie hier ? in unterschiedlicher Weise rechtliche Verantwortungen für unterschiedliche Internet-Adressen treffen.

cc. Soweit der Senat in seinem Beschluss vom 14.06.07 im Zusammenhang mit einem Antrag auf einstweilige Einstellung der Zwangsvollstreckung zu der Frage der Unbestimmtheit (bzw. Reichweite) des Unterlassungstenors eine abweichende Auffassung vertreten hatte, hält der Senat hieran nach nochmaliger Prüfung der Sach- und Rechtslage nicht mehr fest. Ein nicht auf einen bestimmten Dienst beschränktes ? allgemeines ? Verbot kommt auch aufgrund der Besonderheiten der Entscheidung nicht in Betracht. Denn die Unterlassungspflicht der Antragsgegner in dem konkret tenorierten Umfang rechtfertigt sich ? wie im Einzelnen noch auszuführen sein wird ? aus der fehlenden rechtlichen Schutzwürdigkeit ihres Geschäftsmodells im Rahmen des Dienstes www...com. Die insoweit im Rahmen einer Gesamtbetrachtung gemachten Ausführungen lassen sich nicht ohne weiteres auf ein Handeln der Antragsgegner im Rahmen eines anderen Online-Dienstes übertragen. Dieser bedarf vielmehr einer gesonderten Betrachtung jeweils im konkreten Einzelfall.

d. Im Hinblick auf die gewählte Antragsformulierung erfasst dieser jede Art von Verletzungshandlungen. Für Rechtsverletzungen außerhalb des Internets fehlt es allerdings von vornherein an einer Begehungsfahr. Das Geschäftsmodell der Antragsgegner ist ersichtlich allein auf das Internet ausgerichtet. Nur insoweit haben die Antragsgegner eine Begehungsfahr gesetzt. Anhaltspunkte dafür, dass die Antragsgegner außerhalb elektronischer Medien Urheberrechtsverletzungen begehen bzw. hierfür Rahmenbedingungen unterhalten könnten, sind weder von der Antragstellerin vorgetragen worden noch sonst ersichtlich. Unberechtigt sind die Beanstandungen der Antragsgegner deshalb insoweit, als die Antragsfassung auch auf der Grundlage des zweitinstanzlich geänderten Antrags zu 1. ein Verbot ohne die Beschränkung auf elektronische Medien,

etwa durch den Zusatz "im Rahmen eines Online-Dienste" (wie sie diesen nunmehr in den Antrag zu 2. aufgenommen hat) begehrt.

6. Der Antragsgegner zu 2. ist als Verwaltungsrat der Antragsgegnerin zu 1. auch für die dieser Antragsgegnerin zur Last gelegten Rechtsverletzungen unter der Domainadresse www...com passiv legitimiert. Als Verwaltungsrat einer schweizerischen Gesellschaft hat er gem. Art. 716 Abs. 1 Nr. 1 OR die "unübertragbare und unentziehbare" Aufgabe zur "Oberleitung der Gesellschaft und (die) Erteilung der nötigen Weisungen". Er ist weiterhin gem. § 718 Abs. 1 OR allein vertretungsbefugt. In dieser Rechtsstellung ist er mit dem Geschäftsführer einer deutschen GmbH vergleichbar, sodass die hierauf von der Rechtsprechung entwickelten Grundsätze entsprechend anwendbar sind.

7. Die Antragsgegner sind als sog. "Host"-Provider nach § 7 Abs. 2 Satz 2 TMG i. V. m. den allgemeinen gesetzlichen Vorschriften für Rechtsverletzungen verantwortlich, die mittels des von ihnen zur Verfügung gestellten Dienstes begangen werden. In Betracht kommen insoweit insbesondere Urheberrechtsverletzungen gemäß §§ 97 Abs. 1, 19 a UrhG. Eine Haftungsprivilegierung als Diensteanbieter für fremde Informationen gemäß § 10 Satz 1 TMG können die Antragsgegner nicht für sich in Anspruch nehmen.

a. Die Aktivitäten der Antragsgegner sind dadurch gekennzeichnet, dass sie einen reinen Webhosting-Dienst betreiben. Es ist nichts dafür ersichtlich, dass sich die Antragsgegner fremde Inhalte zu Eigen machen (wollen). Nach der gesetzlichen Begründung (BT-Drucks. 13/7385) ist es einem solchen Diensteanbieter "aufgrund der technisch bedingten Vervielfachung von Inhalten und der Unüberschaubarkeit der in ihnen gebundenen Risiken von Rechtsverletzungen zunehmend unmöglich (ist), alle fremden Inhalte im eigenen Dienstbereich zur Kenntnis zu nehmen und auf ihre Rechtmäßigkeit zu prüfen". Diesen Umstand hat der Gesetzgeber zwar zum Anlass für die sich aus § 10 Satz 1 Nr. 1 TMG ergebende Privilegierung des reinen Webhosting-Dienstes genommen. Diese gesetzgeberische Intention beschreibt und beschränkt aber zugleich auch Prüfungspflichten des Diensteanbieters.

b. Diese Privilegierung erstreckt sich indes nicht auf die hier allein streitgegenständlichen Unterlassungsansprüche. Wie sich aus dem Gesamtzusammenhang der gesetzlichen Regelung ergibt, findet die Haftungsprivilegierung des § 10 TMG keine Anwendung auf Unterlassungsansprüche. Dieser Grundsatz kommt zwar im Wortlaut des § 10 TMG nicht vollständig zum Ausdruck, ergibt sich aber u. a. mittelbar aus dem ? für alle Diensteanbieter geltenden ? § 7 Abs. 2 Satz 2 TMG sowie aus Art. 14 der durch diese Vorschriften umgesetzten RL 2000/31/EG, die ausschließlich das Hosting betrifft, dort insbesondere Erwägungsgrund 48 (BGH WRP 07, 1173, 1175 ? Jugendgefährdende Medien bei X; BGH

WRP 07, 964, 966 ? Internet-Versteigerung II; BGH WRP 04, 1287, 1290 ? Internet-Versteigerung I). Wie sich aus der 7 Abs. 2 TMG und dem Gesamtzusammenhang der gesetzlichen Regelung ergibt, betrifft § 10 TMG lediglich die strafrechtliche Verantwortlichkeit und die Schadensersatzhaftung (BGH Urt. V. 27.03.07, VI ZR 101/06).

c. An dieser ? insbesondere im Schrifttum auf Kritik gestoßen ? Rechtsprechung ist festzuhalten. Zur rechtlichen Verantwortlichkeit von Diensteanbietern hatte der Senat in seiner Entscheidung "Chefkoch" (Senat MD 08, 370 ? Chefkoch) u. a. ausgeführt:

"Gegenüber ihrer Inanspruchnahme auf Unterlassung aus §§ 97 Abs. 1, 19a UrhG können sich die Beklagten schon aus rechtssystematischen Gründen nicht auf die Privilegierung des Diensteanbieters für fremde Informationen gemäß § 10 TMG berufen. Denn diese Vorschrift erfasst nur Schadensersatzansprüche, findet jedoch auf Unterlassungsansprüche keine Anwendung. Dies hat der BGH zu der inhaltsgleichen Vorgängernorm (§ 11 Satz 1 TDG) ausdrücklich festgestellt (BGH WRP 04, 1287, 1290 ? Internet-Versteigerung). An dieser inzwischen gefestigten Rechtsprechung (BGH GRUR 07, 724, 730 ? Meinungsforum) ist festzuhalten (BGH GRUR 07, 707, 709 ? Internet-Versteigerung II). Dementsprechend findet insoweit die Vorschrift aus § 7 Abs. 2 TMG keine Anwendung, da auch die §§ 8, 9 TMG nicht einschlägig sind."

8. Die Antragsgegner sind mithin grundsätzlich als Betreiber eines Teledienstes rechtlich (mit)verantwortlich für rechtswidrige Nutzungshandlungen, die über ihren Dienst vorgenommen werden. Über den Dienst der Antragsgegner werden durch das Hochladen, Speichern und Weiterverbreiten nicht autorisierter Programmkopien urheberrechtlich geschützter Software der Antragstellerin durch dritte Nutzer in erheblichem bzw. nicht nur unerheblichem Umfang Urheberrechtsverletzungen zulasten der Antragstellerin begangen. Dieser Umstand steht zwischen den Parteien nicht im Streit. Die Antragsgegner sind jedenfalls dann als Störer hierfür verantwortlich, wenn die insoweit von der Rechtsprechung für die Störerhaftung entwickelten Voraussetzungen erfüllt sind. Dies ist hier der Fall.

a. Als Störer haftet derjenige auf Unterlassung, der ? ohne Täter oder Teilnehmer zu sein ? in irgendeiner Weise willentlich und adäquat kausal zur Verletzung eines geschützten Rechtsguts beiträgt (BGH GRUR 07, 708, 711 ? Internet-Versteigerung II; BGH WRP 04, 1287, 1291 ? Internet-Versteigerung I; BGHZ 148, 13, 17 ? ambiente.de; BGH GRUR 02, 618, 619 ? Meißner Dekor). Weil die Störerhaftung nicht über Gebühr auf Dritte erstreckt werden darf, die nicht selbst die rechtswidrige Beeinträchtigung vorgenommen haben, setzt die Haftung des Störers die Verletzung von Prüfungspflichten voraus. Deren Umfang bestimmt sich danach, ob und inwieweit dem als Störer in Anspruch Genommenen nach den Umständen des Einzelfalls eine Prüfung zuzumuten ist (BGH GRUR 07, 708, 711 ?

Internet-Versteigerung II; BGH WRP 04, 1287, 1292 ? Internet-Versteigerung I; BGH GRUR 97, 313, 315 ? Architektenwettbewerb; BGH GRUR 94, 841, 842 ? Suchwort; BGH GRUR 99, 428, 419 ? Möbelklassiker; BGHZ 148, 13, 17 f ? ambiente.de).

b. Für die Beurteilung der im vorliegenden Rechtsstreit zu entscheidenden Rechtsfragen aus dem Bereich des Urheber- und Markenrechts ist weiterhin von den Grundsätzen der Störerhaftung auszugehen.

aa. Für den Bereich des Wettbewerbsrechts hatte der Bundesgerichtshof in einer aktuellen Entscheidung indes ? hiervon abweichend ? in bestimmten Fällen die täterschaftliche Verantwortlichkeit des Betreibers unter dem Gesichtspunkt der Verletzung einer Verkehrspflicht angenommen.

aaa. Derjenige, der durch sein Handeln im geschäftlichen Verkehr in einer ihm zurechenbaren Weise die Gefahr eröffnet, dass Dritte Interessen von Marktteilnehmern verletzen, die durch das Wettbewerbsrecht geschützt sind, kann eine unlautere Wettbewerbshandlung begehen, wenn er diese Gefahr nicht im Rahmen des Möglichen und Zumutbaren begrenzt (BGH WRP 07, 1173, 1175 ? Jugendgefährdende Medien bei X). Ist dem Betreiber bekannt, dass Anbieter unter Nutzung seiner Plattform mit konkreten Angeboten Rechtsverletzungen begehen, ist sein Verhalten wettbewerbswidrig, wenn er es unterlässt, im Hinblick auf die ihm konkret bekannt gewordenen Verstöße zumutbaren Vorkehrungen zutreffen, um derartige Rechtsverletzungen künftig so weit wie möglich zu verhindern und es infolge dieses Unterlassens entweder zu weiteren derartigen Verstößen von Anbietern kommt oder derartige Verstöße ernsthaft zu besorgen sind (BGH WRP 07, 1173, 1175 ? Jugendgefährdende Medien bei X). Wer durch sein Handeln im geschäftlichen Verkehr die Gefahr schafft, dass Dritte durch das Wettbewerbsrecht geschützte Interessen von Marktteilnehmern verletzen, ist wettbewerbsrechtlich dazu verpflichtet, diese Gefahr im Rahmen des Möglichen und Zumutbaren begrenzen (BGH WRP 07, 1173, 1177 ? Jugendgefährdende Medien bei X). Insoweit kommt eine Haftung nach § 3 UWG unter dem Aspekt der Verletzung einer wettbewerbsrechtlichen Verkehrspflicht in Betracht (BGH WRP 07, 1173, 1177 ? Jugendgefährdende Medien bei X).

bbb. Im Bereich deliktischen Haftung nach § 823 Abs. 1 BGB sind Verkehrspflichten als Verkehrssicherungspflichten in ständiger Rechtsprechung anerkannt. Verkehrspflichten hat der Bundesgerichtshof auch bereits im Immaterialgüterrechten sowie der Sache nach dem Wettbewerbsrecht angenommen (vgl. BGH GRUR 84, 54, 55 ? Kopierläden, für das Urheberrecht; BGH GRUR 95, 601 ? Bahnhofs-Verkaufsstellen, für das Wettbewerbsrecht). Dieser Rechtsprechung aus unterschiedlichen Rechtsbereichen ist der allgemeine

Rechtsgrundsatz gemeinsam, dass jeder, der in seinem Verantwortungsbereich eine Gefahrenquelle schafft oder andauern lässt, die ihm zumutbaren Maßnahmen und Vorkehrungen treffen muss, die zur Abwendung der daraus Dritten drohenden Gefahren notwendig sind (BGH WRP 07, 1173, 1177 ? Jugendgefährdende Medien bei X).

ccc. Wer gegen eine wettbewerbsrechtliche Verkehrspflicht verstößt, ist Täter einer unlauteren Wettbewerbshandlung (BGH WRP 07, 1173, 1177 ? Jugendgefährdende Medien bei X). Der Annahme wettbewerbsrechtlicher Verkehrspflichten steht nicht entgegen, dass diese auf die Abwehr der Beeinträchtigung wettbewerbsrechtlich geschützter Interessen von Marktteilnehmern gerichtet sind und damit auf die Abwendung eines Verhaltens. Die Verkehrspflichten wurden zwar im Rahmen von § 823 Abs. 1 BGB zur Abwendung eines Erfolgsunrechts, nämlich einer Rechtsverletzung entwickelt. Der Rechtsgedanke der Verkehrspflichten, dass der Verantwortung für eine Gefahrenquelle in den Grenzen der Zumutbarkeit eine Pflicht zu gefahrverhütenden Maßnahmen entspricht, gilt aber unabhängig davon, ob sich die Gefahr in einem Erfolgs- oder in einem Handlungsunrecht realisiert (BGH WRP 07, 1173, 1177 ? Jugendgefährdende Medien bei X).

bb. Anlass für diese differenzierte Betrachtung des Bundesgerichtshofs ist nach dem Verständnis des Senats eine ? in früheren Entscheidungen bereits angedeutete ? unterschiedliche Beurteilung der Verantwortlichkeit im Falle eines Erfolgsunrechts (bei absoluten Schutzrechten) bzw. des Handlungsunrechts (bei Wettbewerbsverstößen).

aaa. Soweit in der Rechtsprechung eine gewisse Zurückhaltung gegenüber dem Institut der Störerhaftung zum Ausdruck kommt und erwogen wird, die Passivlegitimation für den Unterlassungsanspruch allein nach den deliktischen Kategorien der Täterschaft und Teilnahme zu begründen (BGHZ 155, 189, 194 f ? Buchpreisbindung; BGH GRUR 03, 969, 970 ? Ausschreibung von Vermessungsleistungen), betrifft dies Fälle des Verhaltensunrechts, in denen keine Verletzung eines absoluten Rechts in Rede steht. Dies ist dann der Fall, wenn ein Betreiber in seinem eigenen geschäftlichen Interessen eine allgemein zugängliche Plattform geschaffen hat, deren Nutzung in nahe liegender Weise mit der Gefahr verbunden ist, schutzwürdige Interessen von Verbrauchern zu beeinträchtigen (BGH WRP 07, 1173, 1175 ? Jugendgefährdende Medien bei X).

bbb. Denn für den Fall einer wettbewerbsrechtlichen Situation kommt nach der Rechtsprechung des BGH eine Verantwortlichkeit aus unmittelbarer Handlungstäterschaft nicht in Betracht. Richtet sich ein gesetzliches Handlungsge- bzw. verbot z. B. an den Anbieter bestimmter Produkte, so verstößt der Betreiber eines Internetdienstes nicht selbst dadurch gegen das Verbot, dass er den Anbietern seine Plattform zur Verfügung stellt und

dort rechtsverletzende Produkte veröffentlicht werden können. Der Betreiber bietet diese Produkte nicht selbst an (BGH WRP 07, 1173, 1175 ? Jugendgefährdende Medien bei X). Eine Haftung als Teilnehmer scheidet ebenfalls aus. Die allein in Betracht zuziehende Hilfestellung setzt zumindest einen bedingten Vorsatz voraus, der das Bewusstsein der Rechtswidrigkeit einschließt muss. Nimmt der Betreiber die Angebote vor Veröffentlichung nicht zur Kenntnis, sondern werden diese im Rahmen eines automatisierten Verfahrens durch den Anbieter selbst ins Internet gestellt, scheidet eine vorsätzliche Teilnahme des Betreibers aus. Der Betreiber hat keine Kenntnis von konkret drohenden Haupttaten, so dass es an dem erforderlichen Gehilfenvorsatz fehlt (BGH WRP 07, 1173, 1175 ? Jugendgefährdende Medien bei X; BGH WRP 04, 1287, 1291 ? Internet-Versteigerung I).

cc. Demgegenüber hatte der Bundesgerichtshof insbesondere in seinen Entscheidungen "Internet-Versteigerung I" und "Internet-Versteigerung II" die Verantwortlichkeit bei der Verletzung absoluter Schutzrechte auf das Haftungsmodell der Störerhaftung gestützt.

aaa. Im Falle der Verletzung von Immaterialgüterrechten, die als absolute Rechte auch nach § 823 Abs. 1, § 1004 BGB Schutz genießen, sind die Grundsätze der Störerhaftung uneingeschränkt anzuwenden (BGH WRP 04, 1287, 1292 ? Internet-Versteigerung I). Denn auch die nicht unmittelbar selbst handelnde Person unterliegt unmittelbar den gegenüber jedermann wirkenden Verbotsbestimmungen zum Schutz der absoluten Schutzrechte (vgl. zur Abgrenzung BGH GRUR 03, 969 ff ? Ausschreibung von Vermessungsleistungen).

bbb. In der Literatur ist die Auffassung vertreten worden, dass eine derartige Unterscheidung nicht aufrechtzuerhalten ist. Eine Grenzlinie zwischen die Immaterialgüterrechte und das UWG zu legen und dabei zu insinuieren, dass es um die Grenze zwischen Erfolgsunrecht und Verhaltensunrecht geht, werde dem Stand der dogmatischen Erkenntnisse zum allgemeinen Deliktsrecht nicht gerecht (Ahrens WRP 07, 1281, 1286). Zwischen der Störerhaftung nach UWG und der Störerhaftung im Immaterialgüterrecht gäbe es keinen strukturbedingten Unterschied (Ahrens, a. a. O., S. 1287; siehe auch Köhler GRUR 08, 1, 7: "Scheinproblem"). Hierfür spricht u. a. auch, dass der Bundesgerichtshof selbst in der Entscheidung "Jugendgefährdende Medien bei X" unter Bezugnahme auf seine zum Urheberrecht ergangene Entscheidung "Kopierläden" (BGH GRUR 84, 54, 55 ? Kopierläden) auf die auch in diesem bereits entwickelte Rechtsprechung zu Verkehrspflichten hingewiesen hatte.

ccc. Gleichwohl hält der Bundesgerichtshof offensichtlich auch weiterhin an dieser Differenzierung fest, wie der Entscheidung "Internet-Versteigerung III" vom 30. April 2008 (I ZR 73/05) zu entnehmen ist. In dieser Entscheidung hat der Bundesgerichtshof ausgeführt:

"Als Störer kann bei der Verletzung absoluter Rechte auf Unterlassung in Anspruch genommen werden, wenn er ? ohne Täter oder Teilnehmer zu seinen ? in irgendeiner Weise willentlich und adäquat kausal zur Verletzung des absoluten Rechts beiträgt (BGH ? Internet-Versteigerung III, Rdnr. 50; Unterstreichungen durch den Senat).

Zwar hat sich der Bundesgerichtshof hierbei nicht von seiner Entscheidung "Jugendgefährdende Medien bei X" abgegrenzt, sodass die in der Literatur zunehmend erwartete (siehe etwa Leistner/Stang WRP 08 533, 541) klare dogmatische Einordnung für alle Fallkonstellationen noch aussteht. Im Hinblick auf die ausdrückliche Bezugnahme auf "absolute Rechte" geht der BGH indes erkennbar weiterhin von einem differenzierten Modell der Verantwortlichkeit aus. Dem schließt sich der Senat für den vorliegenden Rechtsstreit an.

ddd. Für die Entscheidung des vorliegenden Rechtsstreits ergeben sich hieraus jedoch ohnehin keine abweichenden Konsequenzen. Denn sowohl bei der Störerhaftung als auch bei der Täterhaftung in Bezug auf Verkehrspflichten kommt es im Endeffekt entscheidend darauf an, ob die in Anspruch genommene Personen gegen zumutbare Prüfungspflichten verstoßen hat. Im Hinblick hierauf wird im Folgenden verbreitet auch auf die von dem Bundesgerichtshof in der Entscheidung "Jugendgefährdende Medien bei X" aufgestellten Grundsätze Bezug genommen, sofern diese sich nicht materiell von denjenigen unterscheiden, die im Rahmen einer Störerhaftung zu beachten sind. Soweit die unterschiedlichen Haftungsmodelle ? insbesondere bei der Verpflichtung des Täters zur Schadensersatzleistung ? zu gravierend abweichenden Rechtsfolgen führen, sind diese im vorliegenden Verfügungsverfahren nicht relevant.

dd. Zu den allgemeinen Anknüpfungspunkten einer Verantwortlichkeit als Störer für die von dritten Personen begangenen Urheberrechtsverletzungen in Bezug auf einen (möglicherweise) für illegale Zwecke konzipierten, jedoch für illegale Zwecke missbrauchten Dienst hatte der Senat bereits in seiner Entscheidung "Cybersky" (Senat GRUR-RR 06, 148) ausgeführt:

"bb. Der Antragsgegner ist bei der gegebenen Sachlage deshalb nach allgemeinen Grundsätzen Störer einer zu befürchteten Urheberrechtsverletzung. Für eine objektiv rechtswidrige Verletzung eines Urheberrechts ? bzw. deren unmittelbaren Bevorstehen ? ist es ausreichend, dass zwischen dem zu verbietenden Verhalten und dem befürchteten rechtswidrigen Eingriff ein adäquater Ursachenzusammenhang besteht (BGH GRUR 84, 54, 55 ? Kopierläden; BGH GRUR 65, 104, 105 ? Personalausweise/Tonbandgeräte-Händler II), d. h., dass das Verhalten eine nicht hinweg zu denkende Bedingung des Verletzungserfolgs ist. Allein der Umstand, dass ein für

rechtmäßige Zwecke geeignetes Produkt auch zum Rechtsmissbrauch durch Dritte verwendet werden kann, führt allerdings noch nicht zu der Rechtsfolge eines allgemeinen bzw. auf bestimmte Nutzungsarten beschränkten Verbots. Darin ist dem Antragsgegner (allerdings nur) im Ausgangspunkt seiner Argumentation zuzustimmen. Die streitgegenständliche Verletzungshandlung geht indes deutlich weiter.

aaa. Die hier zu klärende Rechtsfrage ist zwar in ihrer konkreten Ausgestaltung neu und ist von der deutschen Rechtsprechung ? soweit ersichtlich ? in dieser Form noch nicht entschieden worden. Allerdings haben vergleichbare Konfliktsituationen zwischen den berechtigten Interessen der Urheber einerseits und Nutzern technischer Neuerungen andererseits bereits in der Vergangenheit die Rechtsprechung beschäftigt. Dies war insbesondere bei der Markteinführung von Tonbandgeräten der Fall. Hierfür sind in der Rechtsprechung Grundsätze entwickelt worden, die auch auf den vorliegenden Fall Anwendung zu finden haben. Danach gilt folgende Rechtslage: Wird ein Medium zur Verfügung gestellt, das neben seiner rechtmäßigen Benutzung auch zu Eingriffen in die Rechte Dritter benutzt werden kann, kommt es maßgeblich darauf an, ob nach objektiver Betrachtung der rechtsverletzende Gebrauch nicht außerhalb aller Wahrscheinlichkeit liegt (BGH GRUR 65, 104, 105 ? Personalausweise/Tonbandgeräte-Händler II) und ob dem Inhaber des Mediums eine Haftung billigerweise zugemutet werden kann. In den im Rechtsleben sehr häufigen Fällen der Lieferung von Stoffen und Geräten, die von den Erwerbern nicht nur zu rechtmäßigem Gebrauch, sondern auch zu Eingriffen in Rechte und Rechtsgüter Dritter benutzt werden können (Gifte, Waffen etc.), kommt es für den Ursachenzusammenhang zwar auch darauf an, ob bei der gebotenen objektiven Betrachtung gerade der rechtsverletzende Gebrauch der Sachen nicht außerhalb aller Wahrscheinlichkeit lag, wobei der Umstand, dass die unmittelbare Rechtsverletzung von einem selbstständig handelnden Dritten vorgenommen wird und der Inhaber des Mediums nur mittelbarer Störer ist, den Ursachenzusammenhang nicht ausschließt (BGH GRUR 84, 54, 55 ? Kopierläden; BGH GRUR 65, 104, 106 ?

Personalausweise/Tonbandgeräte-Händler II). Dies würde aber z. B. auch für Kirchenorgeln oder andere im Wesentlichen für öffentliche Aufführungen bestimmte Musikinstrumente gelten, bei deren bestimmungsgemäßer Verwendung in das dem Urheber vorbehaltene Aufführungsrecht eingegriffen wird, ohne dass dies zu der Folgerung berechtigt, der Lieferant solcher Instrumente setze eine adäquate Ursache für eine etwaige Verletzung des Aufführungsrechts des Urhebers durch den Benutzer des Instruments. Der grundlegende Unterschied liegt darin, dass bei Nutzungshandlungen in der Öffentlichkeit schon angesichts der insoweit bestehenden Kontrollmöglichkeiten für den Regelfall nach der Lebenserfahrung nicht davon ausgegangen werden kann, diese würden ohne die erforderliche Einwilligung des Berechtigten stattfinden. Anders liegt es hingegen, wenn z. B. Instrumente geliefert werden, deren bestimmungsgemäßer Gebrauch in der Regel einen

Eingriff in die Rechte Dritter mit sich bringt, dieser Gebrauch sich aber im privaten Bereich abspielt, der einer wirksamen und der Allgemeinheit zumutbaren Kontrolle weitgehend entzogen ist (BGH GRUR 65, 104, 106 ? Personalausweise/Tonbandgeräte-Händler II). Gerade dann, wenn man den ausschlaggebenden Grund dafür, den Urheber dagegen zu schützen, dass Rechtsverletzungen vorgenommen werden, in dem Umstand erblickt, dass durch die Lieferung eines dazu eingerichteten Mediums die massenhaft stattfindende Vervielfältigung in einer allen Qualitätsansprüchen gerecht werdenden Ausführung von vornherein vom gewerblichen in den privaten Bereich verlagert wird, muss derjenige als für die Verletzung des Urheberrechts mitverantwortlich angesehen werden, der im Rahmen seiner gewerblichen Tätigkeit dem privaten Vervielfältiger das Rüstzeug und die Möglichkeit zur mühelosen Vervielfältigung schafft (BGH GRUR 65, 104, 106 ? Personalausweise/Tonbandgeräte-Händler II)."

Eine entsprechende Situation liegt auch hier vor. Insbesondere bietet der Dienst der Antragsgegner gleichermaßen Gelegenheit für rechtmäßige als auch rechtswidrige Benutzungsformen. Ein rechtsverletzender Gebrauch liegt auch nicht außerhalb aller Wahrscheinlichkeit, wie der eigene Sachvortrag der Antragsgegner zu ihren Bemühungen, das Unwesen von Raubkopierer einzudämmen, anschaulich zeigt.

8. Entscheidend ist auf der Grundlage der aktuellen BGH-Rechtsprechung danach für eine Inanspruchnahme des Störers auf Unterlassung, ob es der Betreiber unterlassen hat, im Hinblick auf die ihm konkret bekannt gewordenen Verstöße wirksame Vorkehrungen zu treffen, um derartige Rechtsverletzungen durch technisch mögliche und zumutbare Maßnahmen künftig so weit wie möglich zu verhindern. Diesem Verhaltensgebot sind die Antragsgegner indes nicht gerecht geworden.

a. Maßgeblich hierfür ist nach der bisherigen Rechtsprechung ? hierauf weisen die Antragsgegner zutreffend hin ? eine konkrete Einzelfallbeurteilung unter Einbeziehung aller entscheidungsrelevanten Aspekte des Streitfalls. Die wettbewerbsrechtliche Verkehrspflicht bzw. die Störerverantwortlichkeit eines Telediensteanbieters hinsichtlich rechtsverletzender fremder Inhalte konkretisiert sich als Prüfungspflicht. Voraussetzung einer Haftung des Telediensteanbieters ist daher eine Verletzung derartiger Prüfungspflichten. Deren Bestehen sowie Umfang richtet sich im Einzelfall nach einer Abwägung aller betroffenen Interessen und relevanten rechtlichen Würdigungen. Überspannte Anforderungen dürfen im Hinblick darauf, dass es sich um eine erlaubte Teilnahme am geschäftlichen Verkehr handelt, nicht gestellt werden. Entsprechend den zur Störerhaftung entwickelten Grundsätzen kommt es entscheidend darauf an, ob und inwieweit den in Anspruch genommenen nach den Umständen eine Prüfung zuzumuten ist (BGH WRP 04, 1287, 1292 ? Internet-Versteigerung; BGH GRUR 97, 313, 315 ? Architektenwettbewerb; BGH GRUR

94, 841, 842 ? Suchwort; BGH GRUR 99, 428, 419 ? Möbelklassiker; BGHZ 148, 13, 17 f ? ambiente.de). Damit wird einer unangemessenen Ausdehnung der Haftung für Rechtsverstöße Dritter entgegengewirkt (BGH WRP 07, 1173, 1177 ? Jugendgefährdende Medien bei X).

b. Auszugehen ist dabei zunächst von der Tatsache, dass die Antragsgegner mit ihrem MD5-Filter, dem Vorhalten einer Abuse-Abteilung sowie der Überprüfung der Dateinamen auf bestimmte Worte bzw. Wortkombinationen bereits Maßnahmen ergriffen haben, die geeignet sind, in bestimmten Umfang Rechtsverletzungen aufzuspüren. Dies steht zwischen den Parteien nicht im Streit. Fraglich ist allein, ob sich die Antragsgegner auf diese Maßnahmen beschränken durften oder ob ihnen weitergehende Aktivitäten abzuverlangen sind. In diesem Zusammenhang ist darauf hinzuweisen, dass die weitergehenden Maßnahmen, die die Antragsgegner mit ihrem nach Schluss der mündlichen Verhandlung vorgelegten Schriftsatz vom 10.06.08 beschrieben haben, hierbei keine Berücksichtigung finden können.

aa. Hierbei sind unterschiedliche Beurteilungsparameter zu berücksichtigen. Zunächst haben die etwaigen Verletzungsvorkehrungen der Bedeutung des Schutzgutes Rechnung zu tragen (Ahrens WRP 07, 1281, 1289). Dabei erfordert zum Beispiel die Verhinderung von Rechtsverletzungen an urheberrechtsgeschützter Software möglicherweise ein geringeres Schutzniveau als etwa die Verhinderung der Verbreitung jugendgefährdender Medien. Bei der Beurteilung der Zumutbarkeit von Abwehrmaßnahmen sind im Rahmen der Einzelfallbeurteilung auch die Funktionen des in Anspruch genommenen Verletzers im Kommunikationsprozess zu bedenken (Ahrens, a. a. O., S. 128). In diesem Zusammenhang wird verschiedentlich betont, dass etwa gerade das Provisionsinteresse von X, welches von den getätigten Geschäften unmittelbar profitiere, Anlass für verschärfte Prüfungspflichten sei (OLG Köln CR 08, 41, 43). Weiterhin soll zu berücksichtigen sein, ob bzw. in welchem Umfang der Verletzte eine zumutbare Eigenvorsorge betreiben kann (Ahrens, a. a. O., S. 1290). In gleicher Weise ist das Angewiesensein des Verletzten auf die Inanspruchnahme des Störers bzw. Trägers von Verkehrspflichten ebenfalls ein maßgeblicher Zurechnungsfaktor. Dem von einem Verletzungsgeschehen Bedrohten ist oftmals nicht damit geholfen, theoretisch gegen zahlreiche, schwer ermittelbare unmittelbare Verletzer vorgehen zu können. Wirksamer Abwehrschutz setzt in diesen Fällen ein Vorgehen gegen denjenigen voraus, der die notwendige Infrastruktur für die Begehung der Rechtsverletzungen im Internet zur Verfügung stellt (vgl. Ahrens, a. a. O., S. 1288; Köhler GRUR 08, 1, 4).

bb. Nach der Rechtsprechung des Bundesgerichtshofs dürfen dem in Anspruch genommenen Verletzer auch keine Anforderungen auferlegt werden, die ein von der

Rechtsordnung gebilligtes Geschäftsmodell gefährden oder seine Tätigkeit unverhältnismäßig erschweren (BGH WRP 07, 1173, 1177 ? Jugendgefährdende Medien bei X). Nach § 7 Abs. 2 TMG, der Art. 15 Abs. 1 der Richtlinie 2000/31/EG in das deutsche Recht umgesetzt, sind Diensteanbieter insbesondere nicht verpflichtet, die von ihnen übermittelten oder gespeicherten Informationen zu überwachen oder nach Umständen zu forschen, die auf eine rechtswidrige Tätigkeit hindeuten (BGH WRP 07, 1173, 1177 ? Jugendgefährdende Medien bei X). Andererseits kann die Gefährdung des Geschäftsmodells durch Kontrollmaßnahmen auch nicht dazu führen, dass der Rechtsinhaber schutzlos gestellt wird. Bei der Verletzung von Rechtsgütern hoher Bedeutung, insbesondere solchen, deren Zuwiderhandlung strafbewehrt ist, reicht es häufig nicht aus, allein die unmittelbaren Verletzer in Anspruch zu nehmen, die die Rechtsverletzungen begehen. Für außenstehende Anspruchsinhaber wird es allenfalls sporadisch, nicht jedoch systematisch und annähernd umfassend möglich sein, die Anbieter zu identifizieren, die zudem häufig nicht unter ihren richtigen Namen auftreten (BGH WRP 07, 1173, 1178 ? Jugendgefährdende Medien bei X). Die Inanspruchnahme der Anbieter könnte notwendig immer erst nach einer gewissen Zeit zu einer Rücknahme oder Sperrung des Angebots führen, sodass dessen rechtsverletzende Wirkungen eingetreten wäre (BGH WRP 07, 1173, 1178 ? Jugendgefährdende Medien bei X). Durch diesen Umstand ergäben sich empfindliche Lücken im Rechtsschutz (BGH WRP 07, 1173, 1178 ? Jugendgefährdende Medien bei X).

cc. Erforderlich ist deshalb eine Abwägungsentscheidung zwischen den berechtigten Interessen des Rechtsinhabers an einer Vermeidung weiterer gleichartiger Rechtsverletzungen sowie den berechtigten Interessen des Betreibers einer Plattform an einer ? trotz erforderlicher Kontrollmechanismen ? weiterhin wirtschaftlich sinnvollen Geschäftstätigkeit, die im Einklang mit der Rechtsordnung steht. Im Rahmen dieser Abwägung ist zu berücksichtigen, dass die Antragsgegner mit ihren Diensten in erster Linie ihren Nutzern ausschließlich Speicherkapazität zur Übertragung von Dateien zur Verfügung stellen wollen, die Verfügungsmacht bei den Nutzern verbleibt, dass die Antragsgegner den Inhalt der Dateien nicht zur Kenntnis nehmen, und dass die Zweckbestimmung der Dienste keine Veröffentlichung ist. Weiter ist zu berücksichtigen, dass der Dienst der Antragsgegner zwar z. T. kostenpflichtig ist, die Antragsgegner aber ? soweit ersichtlich ? keinen Umsatz in Abhängigkeit zum Datenvolumen bzw. zur Zahl der Uploads bzw. Downloads generieren. Demgemäß profitieren die Antragsgegner nicht in besonderer Weise durch die konkrete Art der beanstandeten Rechtsverletzungen, wobei allerdings weitgehend im Dunkeln bleibt, wie sich das Geschäftsmodell der Antragsgegner, das allein durch die erforderlichen Server mit hohem Aufwand betrieben wird, im Einzelnen finanziert.

dd. Im Rahmen der gebotenen Abwägung der Einzelfallinteressen kann der Umstand, dass

ein Anbieter eine Internet-Plattform zur Verfügung stellt, jedenfalls dann nicht allein Prüfungspflichten begründen, wenn Angebote im Rahmen eines Registrierungsverfahrens automatisch durch den Anbieter ins Internet gestellt und von dem Betreiber vor Veröffentlichung nicht zur Kenntnis genommen werden (BGH WRP 07, 1173, 1178 ? Jugendgefährdende Medien bei X). Dem Betreiber einer solchen Plattform ist nicht zuzumuten, jedes Angebot vor Veröffentlichung im Internet auf eine mögliche Rechtsverletzung zu untersuchen. Dem entspricht die gesetzliche Regelung in § 7 Abs. 2 TMG, die eine entsprechende Verpflichtung ausschließt (BGH WRP 07, 1173, 1178 ? Jugendgefährdende Medien bei X).

ee. Eine Handlungspflicht des Betreibers besteht aber, soweit er selbst oder über Dritte Kenntnis von konkreten rechtsverletzenden Angeboten erhält (BGH WRP 07, 1173, 1178 ? Jugendgefährdende Medien bei X). Ab Kenntniserlangung kann er sich nicht mehr auf seine medienrechtliche Freistellung von einer Inhaltskontrolle der bei ihm eingestellten Angebote berufen. Ist der Betreiber auf eine klare Rechtsverletzung hingewiesen worden, besteht für ihn ein Handlungsgebot (BGH WRP 07, 1173, 1178 ? Jugendgefährdende Medien bei X).

ff. Der Betreiber ist dann aber nicht nur verpflichtet, das konkret rechtsverletzende Angebot, von dem er Kenntnis erlangt hat, unverzüglich zu sperren. Er muss auch Vorsorge dafür treffen, dass es möglichst nicht zu weiteren gleichartigen Rechtsverletzungen kommt. Solche gleichartigen Rechtsverletzungen sind nicht notwendigerweise nur Angebote, die mit den bekannt gewordenen Fällen identisch sind, also z. B. das Angebot des gleichen Artikels durch denselben Nutzer (BGH WRP 07, 1173, 1178 ? Jugendgefährdende Medien bei X). Vielmehr hat der Betreiber unter bestimmten Umständen auch zu verhindern, dass die ihm konkret bekannt gewordenen Angebote erneut ? z. B. durch andere Anbieter ? über seinen Dienst angeboten werden (BGH WRP 07, 1173, 1178 ? Jugendgefährdende Medien bei X). Eine solche Prüfungs- und Überwachungspflicht ist schon deshalb notwendig, weil ansonsten der Anbieter, dessen Angebot gelöscht worden ist, sich ohne weiteres z. B. unter einem anderen Namen wieder registrieren lassen und das Angebot wiederholen könnte (BGH WRP 07, 1173, 1178 ? Jugendgefährdende Medien bei X). Allerdings setzen Prüfungspflichten in diesem Umfang voraus, dass eine derartige Überprüfung nach der Art des konkret zur Verfügung gestellten Mediums auch zumutbar und möglich ist.

gg. Insoweit können erhebliche Unterschiede zwischen einem Internet-Marktplatz wie z. B. X und einem Sharehosting-Service wie "rapidshare.de" bzw. "rapidshare.com" bestehen. Hierauf wird im Folgenden noch näher einzugehen sein. Dies ändert indes nichts daran, dass grundsätzlich eine Verpflichtung besteht, im Rahmen des Zumutbaren in dieser Weise umfassend tätig zu werden. Hierzu fehlt es allerdings noch weitgehend an verlässlichen Kriterien für die einzelnen Internet-Dienste.

aaa. Zu Recht stellt Ahrens (Ahrens WRP 07, 1281, 1288) hierzu fest: "Das Schwergewicht künftiger Rechtsprechung wird auf der Ausbildung der spezifischen Verhaltenspflichten liegen müssen". Das OLG Frankfurt hat kürzlich die Verantwortlichkeit eines (reinen) Access-Providers für den Inhalt von Websites im Internet abgelehnt, zu denen er seinen Kunden Zugang vermittelt (OLG Frankfurt, Beschluss vom 22.01.08, 6 W 10/08). Das Handeln der Antragsgegner geht hierüber aber deutlich hinaus. Das OLG Düsseldorf hat die Verantwortlichkeit des Betreibers eines Internetforums im Hinblick auf die Überwachung der in offenen Diskussionsforen vorkommenden rechtsverletzenden Äußerungen abgelehnt, da der hierfür erforderliche Kontrollaufwand unzumutbar sei (OLG Düsseldorf MMR 06, 618). Insoweit bestand allerdings die Besonderheit, dass sich rechtsverletzende Meinungsäußerungen u. ä. weitgehend jeder verlässlichen Feststellung durch Prüfroutinen entziehen. Dies ist bei rechtsverletzender Software mit Urhebervermerken anders. Auch bezüglich der Sharehosting-Dienste der Antragsgegner gibt es bereits eine obergerichtliche Entscheidung des OLG Köln (OLG Köln CR 08, 41 ff). Das OLG Köln hat in einem von der GEMA betriebenen Verfahren letztlich (weitere) Überprüfungspflichten der Antragsgegner verneint, wobei die Auffassung deutlich zu Tage getreten ist, dass sich das Verfügungsverfahren für eine nähere Befassung mit den technischen Fragen nicht eignet und insoweit gegebenenfalls die Einholung eines Sachverständigengutachtens im Hauptsacheverfahren in Betracht kommt.

bbb. Derartige Prüfungspflichten stehen auch mit § 7 Abs. 2 TMG in Einklang, der die effektive Durchsetzung von Löschungs- und Sperrungsansprüchen nach den allgemeinen Gesetzen gewährleisten soll (BGH WRP 07, 1173, 1178 ? Jugendgefährdende Medien bei X). Diese Vorschrift schließt es in Satz 1 zwar aus, Diensteanbieter zu verpflichten, in den von ihnen gespeicherten Fremdinformationen nach Umständen zu forschen, die auf eine rechtswidrige Tätigkeit hinweisen. Hat ein Betreiber aber Kenntnis von einem konkreten Verstoß einer seiner Nutzer gegen das Urheberrecht, so liegt der Hinweis auf eine rechtswidrige Tätigkeit bereits vor (vgl. BGH WRP 07, 1173, 1178 ? Jugendgefährdende Medien bei X). Nach Abs. 2 Satz 2 dieser Vorschrift bleiben die Verpflichtungen zur Entfernung oder Sperrung der Nutzung von Informationen nach den allgemeinen Gesetzen auch im Falle der Nichtverantwortlichkeit des Diensteanbieters nach den §§ 8 bis 10 unberührt. Um eine derartige Pflicht handelt es sich bei der Verpflichtung des Anbieters, in Bezug auf bekannt gewordene Rechtsverletzer auch künftige gleichartige Handlungen zu unterbinden. Insoweit kann sich der Betreiber nicht darauf beschränken allein "reaktiv" tätig zu werden; in diesen Fällen muss er auch nach den Willen des Gesetzes "pro-aktiv" eingreifen.

hh. Ungeachtet der Tatsache, dass die Parteien nachhaltig darüber streiten, ob bzw. mit

welchem Aufwand den Antragsgegnern eine wirksame Überprüfung der hoch geladenen Dateien möglich ist, kann ihnen im Regelfall grundsätzlich rechtstreuen Verhaltens (zu Ausnahmen sogleich noch eingehend) eine flächendeckende Kontrolle ohne Beschränkung auf einzelne Nutzer, die wirksam bereits vor dem ersten Hochladen einsetzen muss, nicht zugemutet werden. Denn der damit verbundene Aufwand würde möglicherweise das gesamte Geschäftsmodell in Frage stellen. Denn allein über den Dienst www...de werden nach den unbestrittenen Angaben der Antragsgegner (in dem Parallelverfahren 5 U 119/07) täglich ca. 250.000 Dateien hoch geladen. Bei dem Dienst www...de sollen 40 Millionen Dateien, bei dem Dienst www...com sollen bei einem täglichen Upload von ca. 150.000 Dateien insgesamt 28 Millionen Dateien gespeichert sein. Eine wirksame (pro-aktive) "Inhaltskontrolle" übersteigt bei einer derartigen Menge im Regelfall ein noch zumutbar geschuldetes Maß eines Diensteanbieters, wenn dieser im Übrigen erkennbar bemüht ist, die berechtigten Interessen der Rechteinhaber zu wahren.

ii. Soweit der Senat im Rahmen seiner "Cybersky"-Entscheidung (Senat GRUR-RR 06, 148 ? Cybersky) den Anbieter von Software für verpflichtet angesehen hat, wirksame Schutzmechanismen zu installieren, die bereits ein urheberrechtsverletzendes Einspeisen bzw. einen Transport rechtsverletzender Programme ausschließen, lag dieser Entscheidung ein abweichender Sachverhalt zugrunde.

aaa. Im dortigen Fall hatte der Entwickler der Software mehr oder minder unverhohlen sein Produkt zur Begehung urheberrechtswidriger Handlungen angepriesen. Hiervon kann im vorliegenden Fall keine Rede sein. Insbesondere reicht es ? entgegen der Auffassung der Antragstellerin ? für die Übertragung der dort entwickelten Grundsätze nicht aus, dass ein Dienst in einschlägigen Kreisen für das Hoch- und Herunterladen von Raubkopien als geeignet angesehen und hierzu verbreitet benutzt wird.

bbb. Die Antragstellerin hat nichts dafür vorgetragen, dass den Antragsgegnern ein ähnliches Verhalten wie im Fall "Cybersky" zur Last zu legen ist. Insbesondere sind die Äußerungen ihres Mitarbeiters D. O. in den Internet-Foren zu einer derartigen Annahme nicht geeignet. D. O. hatte weder zum Hochladen illegaler Software aufgerufen noch hierzu (verdeckte) Hinweise gegeben. Die Antragstellerin hat nicht darzulegen und glaubhaft zu machen vermocht, dass es sich bei der Äußerung dieses Abuse-Mitarbeiters der Antragsgegner zu der Möglichkeit, bereits einmal gesperrte Dateien durch geringfügige Veränderungen erneut hoch zu laden, um eine gezielt lancierte Anleitung zum Rechtsbruch handelte. Für die Behauptung der Antragstellerin spricht nach dem Eindruck des Senats noch nicht einmal eine überwiegende Wahrscheinlichkeit. Die Antragsgegner haben plausibel dargelegt, dass es in der Vergangenheit bereits mehrfach zu Situationen gekommen ist, in denen unverdächtige Originaldateien (versehentlich) gelöscht worden

sind. Für eine derartige Möglichkeit spricht eine nicht unerhebliche Lebenswahrscheinlichkeit. Aus dieser Äußerung zu schließen, die Antragsgegner billigten nicht nur Urheberrechtsverletzungen, sondern legten diese ihren Nutzern geradezu nahe, überspannt ein lebensnahes Verständnis des Beitrags. Vor diesem Hintergrund hält es der Senat für nachvollziehbar, dass die Äußerung von D. O. (Anlage AS 23 in 5 U 73/07) tatsächlich (nur) den Zweck hatte, welchen die Antragsgegner behauptet haben. Hierfür spricht auch, dass die Äußerung des Mitarbeiters offenbar auf eine Einzelanzeige individuell getätigt worden ist, von dem Adressaten sodann aber (offenbar ohne Wissen der Antragsgegner) in ein öffentliches Forum gestellt worden ist. Diesen Sachverhalt hat D. O. mit eidesstattlicher Versicherung vom 26.03.07 (Anlage AG 9 in 5 U 119/07) glaubhaft gemacht. Für die gegenteilige Darlegung der Antragstellerin spricht keine überwiegende Wahrscheinlichkeit.

9. Soweit die Antragsgegner bereits gegenwärtig ihren Dienst auf das Angebot bestimmter konkret urheberrechtsverletzender Softwareangebote der Antragstellerin überprüfen, sind diese Prüfungen allerdings ersichtlich unzureichend und nicht geeignet, ihren Kontroll- und Prüfungspflichten zu genügen. Die von den Antragsgegnern angebotenen Überprüfungsmechanismen sind sinnvoll und zweckmäßig, können die Antragsgegner jedoch nicht von ihrer Verpflichtung entlasten, nach den obigen Grundsätzen erkannte "Risikodateien" bereits vor dem Hochladen einer inhaltliche Kontrolle zu unterziehen. Denn sie beschränken sich allein auf dem Dateinamen bzw. den konkreten Umfang bzw. die Integrität der Dateien. Was den Umfang ihrer Prüfungspflichten angeht, können sich die Antragsgegner jedenfalls bei diesem eng umgrenzten, ihnen konkret bekannten (bzw. ohne weiteres erkennbaren) Nutzerkreis (der zulasten der Antragstellerin bekannt gewordenen Rechtsverletzer) nicht mehr auf die von ihnen bislang praktizierten Verfahren beschränken. Hinsichtlich dieser Nutzer ist den Antragsgegnern nunmehr eine konkrete inhaltliche Überprüfung abzuverlangen. Denn sie wissen, dass diese Nutzer bereits in der Vergangenheit ihren Dienst für urheberrechtsverletzende Uploads verwendet haben. Sie wissen auch, dass sich diese Nutzer allein durch das Löschen und Sperren der zuvor hoch geladenen rechtsverletzenden Dateien nicht davon haben abhalten lassen, den Dienst www...com der Antragsgegner (für den Dienst www...de gilt nichts anderes) erneut in Anspruch zu nehmen. Dieser Umstand trägt eine erheblich gesteigerte Wahrscheinlichkeit dafür in sich, dass dieselben Nutzer erneut die Dienste zum Upload urheberrechtsverletzender Software missbrauchen werden, von dem nahe liegend auch die Antragstellerin erneut in Bezug auf die streitgegenständlichen Programme betroffen sein kann. Irgendwelche ? und sei es stichprobenhafte ? Untersuchungen des Dateiinhalts nehmen die Antragsgegner hingegen nicht vor. Derartige Überprüfungen sind indes notwendig ? und auch zumutbar -, um künftige Urheberrechtsverletzungen zu vermeiden.

a. Der Hinweis der Antragsgegner in ihren Nutzungsbedingungen, dass sie den Upload rechtsverletzender Inhalte und die Verteilung der hierauf bezogenen Links ausdrücklich missbilligen (Anlage BK 20), ist eine notwendige, nicht jedoch eine hinreichende Maßnahme, um ihren Verpflichtungen gerecht zu werden. Denn es entspricht der allgemeinen Lebenserfahrung, dass sich Rechtsverletzer hiervon nicht abhalten lassen werden, wenn der Dienst ihnen andererseits hervorragende Rahmenbedingungen für ihr beabsichtigtes Verhalten bietet und darüber hinaus wegen der bestehenden Anonymität die Gefahr, auf Sanktionen in Anspruch genommen zu werden, gering ist.

b. Auch die Tatsache, dass die Antragsgegner extra eine Abuse-Abteilung vorhalten, um Rechtsverletzungen über ihre Dienste aufzuspüren und zu vermeiden, ist eine notwendige Reaktion auf die sich aus der Struktur der Dienste ergebenden vielfältigen Missbrauchsmöglichkeiten. Entscheidend ist nicht, ob die Antragsgegner eine derartige Abteilung mit einer Reihe von Mitarbeitern vorhalten, sondern allein, wie deren Aufgabenstellung definiert ist, insbesondere ob die vorgenommenen Aktivitäten ausreichend sind, um den sich rechtlich ergebenden Handlungspflichten gerecht zu werden. Dies ist ersichtlich nicht der Fall.

c. Das hierbei verwendete MD5-Verfahren ist schon deshalb nicht hinreichend geeignet, weil es anderen Zwecken dient.

aa. Es ist durch folgende Funktionsweise gekennzeichnet: Aus einer beliebig langen Folge von Bytes wird ein 16 Bytes langer Wert (sog. MD5-Wert) gebildet, der die Datei identifiziert. Mit diesem Verfahren wird eine Prüfsumme (digitale Signatur bzw. genetischer Fingerabdruck) generiert, mittels derer festgestellt werden kann, ob eine Datei verändert worden ist. Jede zu 100% identische Datei hat stets ein und denselben MD5-Wert. Die Prüfsumme reagiert dabei auch auf kleine Veränderungen (Anlage AS 25). Als identisch erkannte Dateien werden von den Filtern der Antragsgegner als Raubkopien behandelt und automatisch gelöscht. Dieses Verfahren ist aber ungeeignet, sicher auszuschließen, dass gesperrte Dateien erneut hoch geladen werden. Hierfür ist das Verfahren letztlich auch nicht vorgesehen, denn das Verfahren prüft in erster Linie die Integrität einer Datei.

bb. Allerdings trägt die Antragstellerin selbst vor, dass die Änderung von Dateien zur Umgehung des MD5-Filter gerade bei ausführbaren Computerprogrammen (z. B. *.exe-Dateien) äußerst (zeit)aufwändig ist und dem Ziel der Raubkopierer-Szene widerspricht, identische Kopien kommerzieller Software in Umlauf zu bringen. Selbst wenn eine Überprüfung nach dem MD5-Verfahren für eine Veränderung von Raubkopien nicht vorgesehen ist, könnte dieser Umstand dann zumindest ein Indiz dafür sein, dass das Verfahren jedenfalls deshalb wirkungsvoll ist, weil es Raubkopierer faktisch von einem

Missbrauch abhält. Auch dies ist aber ? wie die von der Antragstellerin vorgetragene wiederholte Einstellung gleichartiger Raubkopien zeigt ? offensichtlich nicht der Fall. Soweit für die Überwindung derartiger Schutzmechanismen vertiefte Computer-Kenntnisse erforderlich sind, sind diese im Übrigen auch bei denjenigen Personen, die illegale Kopien von geschützten Werken über den Dienst der Antragsgegner verbreiten wollen, als vorhanden vorzusetzen. Diese sind in der Regel auch einer Lage, Veränderungen am Dateiinhalt vorzunehmen.

cc. Dies gilt in besonderer Weise für den missbräuchlichen Upload von komplexen Softwareprogrammen, die ? wie auch das streitgegenständliche Programm ? in der Regel für die Ausführbarkeit eine Reihe unterschiedlicher Dateien benötigen. Derartige Programmpakete ? dies ist zwischen den Parteien nicht streitig ? werden von missbräuchlichen Nutzern häufig in gepackte Archive gespeichert und/oder in einzelne Dateipakete zerlegt und später wieder zusammengesetzt. Insbesondere bei diesen ? unstreitig ? in der Raubkopierszene gängigen Vorgehensweisen ist der Einsatz des MD5-Verfahrens ersichtlich wirkungslos. Denn eine Veränderung des MD5-Werts lässt sich problemlos z. B. schon damit bewirken, dass einfach eine zusätzliche (z. B. leere oder mit bedeutungslosen Zeichen versehene) *.txt-Datei in das Archiv mit eingebunden wird, die funktionslos ist und später gelöscht oder schlicht ignoriert werden kann. Bereits hierdurch ergibt sich ein veränderter MD5-Wert. Ein auch nur annähernd geeigneter Schutz der Interessen der Urheberrechtsberechtigten kann durch dieses Verfahren deshalb nicht bewirkt werden.

dd. Vor diesem Hintergrund kommt es nicht entscheidend darauf an, dass die Antragsteller-Vertreter in dem Rechtsstreit 5 U 149/07 dargelegt haben, es sei ihnen kurz vor dem Kammertermin des Landgerichts gelungen, eine Datei mit der Bezeichnung des rechtsverletzenden Programms im Dateinamen in den Dienst www...com hoch zu laden. Die Datei sei von dem MD5-Filter nicht erkannt bzw. abgefangen worden, woraus die Antragstellerin den Schluss zieht, die Antragsgegner hätten entsprechende Vorsorge gar nicht getroffen, weil der MD5-Wert beider Uploads identisch gewesen sei. Den Gründen hierfür muss der Senat für die Entscheidung dieses Rechtsstreits nicht nachgehen.

d. Das Verfahren ist zwar um einen Wortfilter ergänzt, der Dateinamen auf bestimmte Schlüsselwörter durchsucht. Auch diese Überprüfung ist indes unzureichend.

aa. Zwar hatte die Antragstellerin in dem beigezogenen Parallelrechtsstreit 5 U 149/07 dargelegt, dass die rechtsverletzende Software dort bereits durch eine einfache Kontrolle des Dateinamens im Link bei dem Dienst www...com zu erkennen gewesen wäre. Denn der Dateilink lautet jeweils: "...com/files/.../sametime-connect-win-7.5.0.rar", wobei die Begriffe

"Connect" und "7.5" ebenfalls Teil der Produktbezeichnung sind.

bb. Es spricht indes keinerlei Wahrscheinlichkeit dafür, dass rechtsverletzende Kopien stets oder nur in einer überwiegenden Zahl von Fällen die Produktbezeichnung oder Teile von ihr im Dateinamen tragen. Das Gegenteil ist der Fall. Gerade wenn Raubkopierer eine Entdeckung ihrer Aktivitäten mit großem Aufwand zu verhindern suchen, liegt es fern, bereits in dem Dateinamen Hinweise auf ihre Rechtsverletzung zu verankern. Deswegen kann ein solches Verfahren weder für sich genommen noch in Verbindung mit dem MD5-Filter ausreichend sein, um künftige Rechtsverletzungen zu unterbinden. Hieran ändert auch der Umstand nichts, dass in der Vergangenheit eine Vielzahl von Dateien über diesen Wortfilter als verdächtig aussortiert worden sind.

cc. Ebenfalls zutreffend ist der Rechtsstandpunkt der Antragsgegner in dem Parallelrechtsstreit 5 U 119/07, dass allein die Verwendung bestimmter Schlüsselbegriffe ? wie Lotus oder IBM ? im Dateinamen nicht hinreichend geeignet ist, die Vermutung einer konkreten (Urheberrechts)Verletzung zu begründen, die den Antragsgegnern zu konkreten inhaltlichen Überprüfungen der Dateien veranlassen muss. Derartige Prüfungspflichten setzen voraus, dass die Antragstellerin einen konkreten Rechtsverstoß dargelegt hat. Eine Verdachtsprüfung ist von dem Antragsgegner nicht geschuldet. Die Verwendung bestimmter Schlüsselworte in Dateinamen kann zwar einen Hinweis auf rechtsverletzende Nutzungen geben, kann aber auch andere Hintergründe haben. Die Antragsgegner haben zudem unter Vorlage der Anlagen BK 1 und BK 2 dargelegt, dass es ein Produkt der Antragstellerin gibt, das kostenlos verfügbar ist, auf welches aber gleichwohl beide Schlüsselbegriffe zutreffen ("IBM Lotus Symphonie"). Deshalb ist eine derartige Art der Überprüfung nicht geeignet, Rechtsverletzungen mit Wahrscheinlichkeit zu verhindern.

e. Die Kontrolle einer Vielzahl von Raubkopierer-Websites durch Mitarbeiter der Antragsgegner ist gleichermaßen zwar eine angemessene und sinnvolle Überwachungsmethode, die jedoch ebenfalls eine wirksame Verhinderung von Rechtsverletzungen nicht gewährleisten kann.

aa. Das von der Antragstellerin diskutierte "Website-Monitoring" in Bezug auf für den Umschlag von Raubkopien bekannte Internet-Seiten (nach ihren Angaben in der Vergangenheit 604 Seiten) ist eine vernünftige Maßnahme, setzt jedoch erst dann ein, wenn eine Urheberrechtsverletzung bereits stattgefunden hat. Eine derartige Maßnahme kann allenfalls unterstützende Funktion haben. Die allgemeine Verpflichtung einer pro-aktiven Kontrolle solcher Seiten, um Rechtsverletzungen aufzuspüren, mit denen zu rechnen die Antragsgegner bislang keinen konkreten Anlass hatten, obliegt ihnen entgegen der Auffassung der Antragstellerin nicht. Im Übrigen sind die Antragsgegner nicht

verpflichtet, eine möglichst große (aber notwendigerweise unvollständige) Zahl potenzieller Verletzungsfälle zu ermitteln (und zu verhindern), sondern bei denjenigen Nutzern, bei denen ihnen konkrete Prüfungspflichten obliegen, weitere Verletzungsfälle sicher zu verhindern.

bb. Gleichwohl ist es in hohem Maße sinnvoll, wenn die Antragsgegner ? wie auch bisher ? z. B. derartige Seiten aktiv regelmäßig überprüfen, allein deshalb, um dem Missbrauch ihres Dienstes, aus dem ihnen ein erheblicher Überprüfungsaufwand erwächst, wirksam einen Riegel vorzuschieben. Die Auffassung des OLG Köln (OLG Köln CR 08, 41, 42, 43), welches die Überprüfung derartiger Raubkopierer-Seiten für die einzige den Antragsgegnern konkret zuzumutende Maßnahme angesehen hat, teilt der Senat indes nicht. In rechtlicher Hinsicht ist diese Maßnahme unzureichend, wenngleich in tatsächlicher Hinsicht wünschenswert. Denn zu dem Zeitpunkt, zu dem derartige Links in der "Szene" publiziert werden, ist die Rechtsverletzung bereits eingetreten. Die Raubkopien sind hoch geladen und ihr Speicherort der interessierten Öffentlichkeit zugänglich gemacht worden. Ein derartiges Verhalten kommt für einen effektiven Rechtsschutz zu spät. Anders ausgedrückt: Die Antragsgegner mögen ? um es bildlich auszudrücken ? auch gehalten sein, nachträglich ein Kind zu retten zu versuchen, das in einen von ihnen eröffneten, nicht hinreichend gesicherten Brunnen gefallen ist. In rechtlicher Hinsicht sind die Antragsgegner indes in erster Linie verpflichtet, wirkungsvoll zu verhindern, dass das Kind überhaupt in den Brunnen fallen kann. Soweit in der Rechtsprechung (OLG Köln CR 08, 41 ff) derartige Maßnahmen für ausreichend angesehen worden sind, vermag sich der Senat dem nicht anzuschließen.

f. Gleiches gilt für die von den Antragsgegnern verschiedenen Rechteinhabern eingeräumte Möglichkeit eines Zugangs zu dem von ihnen genutzten Löschoberfläche. Zwar wäre es sinnvoll, wenn die Antragstellerin von dieser Option Gebrauch machen würde. Durch eine derartige Möglichkeit der Selbsthilfe verringern sich indes die den Antragsgegnern obliegenden Überprüfungspflichten nicht in einem im Rahmen des vorliegenden Rechtsstreits erheblichen Umfang. Der Senat teilt die in der Senatsverhandlung von den Antragsgegnern wiederholte Auffassung nicht, Rechteinhaber wie die Antragstellerin seien in erheblichem Umfang zur "Eigenvorsorge" verpflichtet; die Tatsache, dass die streitgegenständliche Software nicht über einen wirksamen Kopierschutz verfüge, gereiche der Antragstellerin bei der Verfolgung ihrer Ansprüche im vorliegenden Rechtsstreit zum Nachteil. Die Verhinderung urheberrechtsverletzender Nutzungen auf den von ihnen zur Verfügung gestellten Diensten obliegt zunächst allein den Antragsgegnern. Diese haben Rechtsverstöße in eigener Verantwortung zu unterbinden. Allenfalls in dem Bereich, in dem Rechtsverstöße trotz zumutbarer Maßnahmen der Betreiber derartiger Dienste nicht vollständig verhindert werden können, kann den Rechteinhabern zulässigerweise

entgegengehalten werden, ein vollständiger Schutz sei nur durch ihre Mitwirkung herzustellen. Die Rechteinhaber sind indes nicht verpflichtet, durch Eigenvorsorge die Antragsgegner von der Erfüllung ihrer notwendigen Prüfungspflichten und Zugangsbeschränkungen zu entlasten.

g. Lediglich der Vollständigkeit halber ist darauf hinzuweisen, dass die von den Antragsgegnern mit Schriftsatz vom 10. Juni 2008 vorgetragene, zivilprozessual ohnehin nicht berücksichtigungsfähigen weiteren Maßnahmen auch inhaltlich nicht geeignet wären, den rechtlichen Anforderungen an Prüfungspflichten zu genügen.

10. Die Prüfungspflicht der Antragsgegner erstreckt sich allerdings im Regelfall entgegen der Auffassung der Antragstellerin nicht auf sämtliche eingestellten Angebote.

a. Die Antragsgegner weisen zu Recht darauf hin, dass durch den Umfang der auferlegten Prüfungspflichten nicht letztlich dasjenige Privileg in das Gegenteil verkehrt werden darf, das § 10 Satz 1 Nr. 1 TMG vorgesehen hat. Konkrete Handlungsobliegenheiten ergeben sich gem. § 10 Satz 1 Nr. 2 TMG erst ab dem Zeitpunkt der Kenntnis des Diensteanbieters von den rechtswidrigen Informationen.

b. Der Betreiber hat nicht alle in seinen Dienst eingestellten Angebote daraufhin zu überprüfen, ob sie sich auf rechtsverletzende Inhalte beziehen (vgl. BGH WRP 07, 1173, 1178 ? Jugendgefährdende Medien bei X). Ebenso wenig trifft ihn ? ohne dass der Senat dies im vorliegenden Fall verbindlich zu entscheiden hat ? notwendigerweise eine Prüfungspflicht für sämtliche Angebote aller derjenigen Nutzer, die bereits durch (irgend)ein rechtswidriges Angebot aufgefallen sind (vgl. BGH WRP 07, 1173, 1179 ? Jugendgefährdende Medien bei X), wenngleich der Bundesgerichtshof zumindest bei der Verbreitung jugendgefährdender Medien ? über das identische Produkt hinaus ? eine Erweiterung auf "Inhalte derselben jugendgefährdenden Kategorie auf demselben Trägermedium" offenbar für denkbar hält (Rdn. 53). Eine auf das gesamte Angebot bezogene Überwachungspflicht wird jedenfalls durch § 7 Abs. 2 Satz 1 TMG ausgeschlossen, der einer derartigen aktiven Suchpflicht entgegensteht (BGH WRP 07, 1173, 1179 ? Jugendgefährdende Medien bei X).

c. Zur Begründung einer Prüfungspflicht bedarf es vielmehr eines konkreten Hinweises auf ein rechtswidriges Angebot eines bestimmten Nutzers. Für eine solche Konkretisierung hinsichtlich der Gesamtheit der Nutzer, die den Dienst des Betreibers nutzen, reicht es im Regelfall nicht aus, dass es in der Vergangenheit bereits derartige Angebote bei anderen Nutzern gegeben hat (BGH WRP 07, 1173, 1179 ? Jugendgefährdende Medien bei X). Ebenso wenig liegt bezüglich eines bestimmten Nutzers eine Konkretisierung der

Rechtsgefährdung auf alle Arten von Rechtsverletzungen schon dann vor, wenn er in der Vergangenheit nur eine bestimmte Art rechtsverletzender Produkte angewiesen hat (BGH WRP 07, 1173, 1179 ? Jugendgefährdende Medien bei X). Hieraus ergibt sich nicht notwendigerweise eine erhöhte Wahrscheinlichkeit dafür, dass er auf andersartige rechtsverletzende Ware anbietet (BGH WRP 07, 1173, 1179 ? Jugendgefährdende Medien bei X).

d. Zu dem danach geschuldeten Umfang von Prüfungspflichten hatte der Senat unter Bezugnahme auf die urheberrechtliche höchstrichterliche Rechtsprechung in der Entscheidung "Cybersky" u. a. ausgeführt:

"a. Wenn ein ? wenn auch möglicherweise nur geringfügiger ? Teil der Erwerber das Medium für Zwecke verwendet, die nicht in Urheberrechte Dritter eingreifen, kann ein generelles Verbot des Vertriebs des Mediums rechtsmissbräuchlich sein (BGH GRUR 65, 104, 107 ? Personalausweise/Tonbandgeräte-Händler II). Der Urheber kann den Vertrieb des Mediums nur von solchen Maßnahmen des Verletzers abhängig machen, die einerseits erforderlich und geeignet sind, die Urheberrechtsgefährdung zu beseitigen, andererseits aber keine unzumutbare Belastung für den Vertreiber bzw. Erwerber des Mediums darstellen (BGH GRUR 65, 104, 107 ? Personalausweise/Tonbandgeräte-Händler II). Hat eine Person die ernsthafte Gefahr einer Verletzung von Urheberrechten durch Dritte in zurechenbarer Weise (mit)verursacht, folgt daraus ihre Verpflichtung, alle zumutbaren Sicherungsmaßnahmen zu treffen, durch die die Gefährdung der Rechte des Urhebers ausgeschlossen oder doch ernsthaft gemindert werden kann (BGH GRUR 84, 54, 55 ? Kopierläden; BGH GRUR 65, 104, 105 ? Personalausweise/Tonbandgeräte-Händler II; BGH GRUR 64, 94, 96 ? Tonbandgeräte-Hersteller). Art und Umfang der Maßnahmen bestimmen sich nach Treu und Glauben. Allgemeine Regeln darüber, welche Sicherungsmaßnahmen zur Verhütung eines rechtsverletzenden Gebrauchs eines Gegenstandes, der seiner Natur nach einen solchen Gebrauch ermöglicht oder sogar nahe legt, notwendig und zumutbar erscheinen, lassen sich nicht aufstellen (BGH GRUR 64, 94, 96 ? Tonbandgeräte-Hersteller). Der Störer ist im Rahmen des Zumutbaren und Erforderlichen verpflichtet ist, geeignete Vorkehrungen zu treffen, durch die die Rechtsverletzung soweit wie möglich verhindert werden können. (BGH GRUR 84, 54, 55 ? Kopierläden; BGH GRUR 65, 104, 105 ? Personalausweise/Tonbandgeräte-Händler II)."

e. Vor diesem Hintergrund obliegt es den Antragsgegnern nicht ? wie von der Antragstellerin gefordert -, vorsorglich ihr gesamtes Angebote nach möglichen, die Antragstellerin rechtsverletzenden Programmkopien der streitgegenständlichen Software zu durchsuchen.

f. Sie sind indes verpflichtet, diejenigen Nutzer, die in der Vergangenheit bereits die hier streitgegenständlichen Programme hochgeladen haben, auch zukünftig intensiv und wirkungsvoll zu überprüfen. Haben die Antragsgegner aufgrund eigener Recherchen ihrer Abuse-Abteilung oder durch Beanstandungen durch die Antragstellerin oder Dritte von einem rechtsverletzenden Angebot durch einen bestimmten Nutzer Kenntnis erlangt, so sind sie verpflichtet, dessen Aktivitäten in Zukunft auf derartige Rechtsverletzungen zugunsten der Antragstellerin zu kontrollieren. Die Erfüllung derartiger Prüfungspflichten ist den Antragsgegnern ohne weiteres zumutbar.

11. Die ausgeführten Grundsätze zu einer Einschränkung der erforderlichen Prüfungspflichten oder der Grundsatz der Zumutbarkeit im Rahmen einer erlaubten Tätigkeit stehen nach der Rechtsprechung des Bundesgerichtshofs indes unter dem ausdrücklichen Vorbehalt, dass der in Anspruch genommene Verletzer "ein von der Rechtsordnung gebilligtes Geschäftsmodell" betreibt und ihm deshalb keine Anforderungen auferlegt werden dürfen, die dieses gefährden oder seine Tätigkeit unverhältnismäßig erschweren (BGH WRP 07, 1173, 1177 ? Jugendgefährdende Medien bei X). Der Bundesgerichtshof weist in derselben Entscheidung aber ausdrücklich auch daraufhin, dass einem Geschäftsmodell andererseits die ernst zu nehmende Gefahr immanent sein kann, dass es für die Begehung von Straftaten und unlauteren Wettbewerbshandlungen genutzt wird. Eine solche Gefahr folgt insbesondere aus einer durch die Möglichkeit zur freien Wahl eines Pseudonyms gewährleisteten Anonymität, der Möglichkeit einer problemlosen Abwicklung im Fernabsatz sowie der typischen, deutlich herabgesetzten Hemmschwelle für potenzielle Nutzer, sich für entsprechende Angebote zu interessieren (BGH WRP 1173, 1175 ? Jugendgefährdende Medien bei X). Ein derartiges Geschäftsmodell kann nach Auffassung des Senats dann, wenn es aufgrund seiner Struktur der massenhaften Begehung zum Beispiel von Urheberrechtsverletzungen Vorschub leistet, nicht von der Rechtsordnung gebilligt werden. Denn damit werden die über Art. 14 GG geschützten Interessen der Schutzrechtsinhaber in einem bestimmten Umfeld letztlich "institutionalisiert" schutzlos gestellt und verletzt. Dies bedeutet im Gegenschluss, dass die von dem BGH zum Schutze des Dienstbetreibers vorgesehenen Einschränkungen der Prüfungspflichten dann nicht Platz greifen können. Auf die nach der Rechtsprechung des BGH im Regelfall bestehende Privilegierung kann sich ein Provider insbesondere dann nicht berufen, wenn er die ihm zumutbaren und nahe liegenden Möglichkeiten, die Identität des Nutzers zum Nachweis einer etwaigen Wiederholungshandlung festzustellen (oder sogar dem Berechtigten eine Rechtsverfolgung gegen diesen Nutzern zu ermöglichen), willentlich und systematisch ungenutzt lässt und damit die Interessen der Schutzrechtsinhaber der Beliebigkeit preisgibt. Ein solches Geschäftsmodell kann von der Rechtsprechung nicht gebilligt werden. In einem derartigen Fall scheidet eine Differenzierung nach zumutbaren und nicht zumutbaren Überprüfungsmaßnahmen aus. In Betracht kommt allein ein

"Generalverbot" in Bezug auf das konkret streitgegenständliche Schutzobjekt. So verhält es sich im vorliegenden Fall.

a. Nach der zutreffenden Auffassung von Flechsig (MMR 02, 347, 348) ist ein derartiger Fall der fehlenden Vorkehrungen zur Identitätsfeststellung dem in § 10 Satz 2 TMG normierten Ausschluss gleichzustellen, wonach das Haftungsprivileg keine Anwendung findet, wenn der Nutzer dem Dienstanbieter untersteht oder von ihm beaufsichtigt wird. Die Weigerung, denjenigen Nutzer, der den Dienst in Anspruch nimmt, überhaupt in einer zumindest theoretisch identifizierbaren Art und Weise zur Kenntnis zu nehmen bzw. die Weigerung oder Unmöglichkeit der Benennung der relevanten IP-Adresse des Nutzers, widerspricht dem Willen des Gesetzgebers zur Haftungsprivilegierung von Diensteanbietern, die Informationen im Sinne von § 10 TMG speichern. Die Frage, ob das Verlangen von Flechsig begründet ist (a. a. O., Seite 349), der sogar die Benennung des Namens und der ladungsfähigen Anschrift für geschuldet hält, bedarf im vorliegenden Rechtsstreit keiner Entscheidung, da die Antragstellerin dies nicht begehrt. Hiergegen wenden Sieber/Höfing (a. a. O., Seite 580) ein, dass § 7 Abs. 2 Satz 2 TMG als Ausnahme der Vorschrift nicht nur eng auszulegen, sondern einer Analogie auch nicht zugänglich ist.

b. Grundsätzlich kann ein Sharehosting-Provider wie die Antragsgegnerin zu 1. durch identifizierbare Angaben ohne weiteres Kenntnis von der Identität ihrer Nutzern bzw. den von ihnen zum Verbindungsaufbau gewählten Computern haben. Es ist ihm deshalb auch möglich, künftige gleichartige Rechtsverletzungen durch wirkungsvolle Kontrollmechanismen bzw. Zugangssperren in einem zumutbaren Ausmaß zu verhindern.

aa. Soweit sich die Nutzer der Antragsgegner bei ihren Diensten anmelden bzw. registrieren lassen, kennen die Antragsgegner deren Namen oder zumindest deren E-Mail-Adressen. Sie können deshalb ohne weiteres reagieren, wenn einer dieser registrierten Nutzer, der in der Vergangenheit durch ein Upload rechtsverletzender Dateien zum Nachteil der Antragstellerin aufgefallen ist, ihren Dienst erneut für das Hochladen potenziell rechtsverletzender Dateien in Anspruch nimmt.

bb. Dieselben Möglichkeiten bestehen auch gegenüber anonymen Nutzern. Von diesen kennen die Antragsgegner zumindest die IP-Adressen, von denen frühere rechtsverletzende Angebote hochgeladen worden sind. Jedenfalls ist es den Antragsgegnern zumutbar, bei anonymen Nutzern vorsorglich für jeden Ladevorgang die IP-Adresse zu registrieren und für einen angemessenen Zeitraum zu speichern. Werden von derselben IP-Adresse nach vorheriger Beanstandung erneut potenziell die Antragstellerin rechtsverletzende Dateien hoch geladen, so sind die Antragsgegner zu konkretem Handeln verpflichtet. Denn sie wissen, dass insoweit eine erheblich gesteigerte

Wahrscheinlichkeit für eine erneute Rechtsverletzung besteht.

cc. Entsprechende Erkenntnismöglichkeiten und Kontrollverpflichtungen bestehen auch in den Fällen, in denen ? wie die Antragsgegner geltend machen ? ausländische Nutzer ihren Dienst über eine IP-Adresse benutzen, die nicht einem einzelnen Nutzer, sondern einer Mehrheit von Nutzern oder sogar einem ganzen Stadtteil zugeordnet ist. Der Senat muss nicht darüber entscheiden, ob es den Antragsgegnern von vornherein zumutbar ist, in derartigen Fällen die IP-Adresse vollständig von der Nutzung zu sperren und damit auch rechtstreue Nutzer von ihrem Angebot auszuschließen. Sofern die Antragsgegner diesen Weg nicht beschreiten wollen, wären sie indes verpflichtet, die ihnen zumutbaren Prüfungsmaßnahmen auf alle diejenigen Uploads zu erstrecken, die über diese IP-Adresse in ihre Dienste eingestellt werden. Der hiermit verbundene Mehraufwand und der Umstand, dass sich darunter möglicherweise auch eine Reihe völlig unverdächtiger Dateien befinden, ist den Antragsgegnerin zumutbar, wenn sie andererseits denjenigen rechtstreuen Nutzern, die eine solche IP-Adresse (mit) nutzen, die wegen rechtsverletzender Aktivitäten bereits aufgefallen ist, den Zugang erhalten wollen.

c. Die Antragsgegner haben auch tatsächlich eine hinreichend konkrete Kenntnis, welche Nutzer bzw. über welche IP-Adresse in der Vergangenheit die Antragstellerin rechtsverletzende Softwareprogramme der streitgegenständlichen Art hochgeladen worden sind bzw. welche Upload-Vorgänge die Antragstellerin insoweit konkret beanstandet hat. Die Antragsgegner haben erstinstanzlich mit ihrer Anlage AG 13 umfangreiche Listen von solchen Upload-Vorgängen vorgelegt, die sie selbst in der Vergangenheit als rechtsverletzend erkannt und registriert haben. Von derartigen Nutzern wissen die Antragsgegner, dass insoweit die erhöhte Wahrscheinlichkeit einer Rechtsverletzung zulasten der Antragstellerin besteht. Zumindest Angebote dieser Nutzer (die möglicherweise nur über eine IP-Adresse identifizierbar sind) hätten die Antragsgegner in der Folgezeit ? und zwar unaufgefordert ? einer Überprüfung auf mögliche Urheberrechtsverletzungen zulasten der Antragstellerin in Bezug auf die streitgegenständlichen Softwareprodukte unterziehen müssen.

d. Trotz eines ausdrücklichen, dahin gehenden Verlangens der Antragstellerin haben sich die Antragsgegner indes in der Vergangenheit nicht dazu bereit gefunden, diese ihnen bekannten Daten der Antragstellerin mitzuteilen, damit diese zur Vermeidung künftiger Rechtsverletzungen überhaupt in die Lage versetzt wird, festzustellen, ob aus einer Quelle erneut eine Rechtsverletzung entspringt. Mit ihrem Schriftsatz vom 21.02.08 hatte die Antragstellerin auf Anfrage des Senats ausdrücklich vorgetragen, dass die Antragsgegner ? mit Ausnahme des ersten Verletzungsfalls ? sogar noch nicht einmal die bisherigen Anfragen der Antragstellerin um Bekanntgabe der rechtsverletzenden IP-Adressen

beantwortet haben. Dieses Verhalten zeigt, dass die Antragsgegner letztlich nicht gewillt sind, das ihnen Mögliche und Zumutbare zu tun, um in Kooperation mit der Antragstellerin künftige Rechtsverletzungen zu unterbinden. Schon dieses Verhalten lässt erhebliche Zweifel daran aufkommen, ob das Geschäftsmodell der Antragsgegner tatsächlich in erster Linie auf rechtmäßige Nutzungsformen ausgerichtet ist. Gerade wenn Einzelpersonen über die IP-Adressen im Regelfall nicht identifizierbar sind, dürften auch Datenschutzerwägungen einer von der Antragstellerin verlangten Bekanntgabe nicht entgegenstehen.

e. Ohnehin hat die Antragstellerin im Fall einer erkannten Rechtsverletzung ? und insoweit grundlegend anders als bei X ? Kenntnis nur von dem Link, zu dem die rechtsverletzenden Dateien hochgeladen worden ist. Die Information, welcher Nutzer dies veranlasst hat bzw. von welcher IP-Adresse dies geschehen ist, haben im Zweifel allein die Antragsgegner. Deshalb ist es der Antragstellerin letztlich unmöglich, den Nachweis einer "Wiederholungstat" zu führen, wenn die Antragsgegnerin ihr die Information über diese Daten verweigern. Die Antragsgegner wären verpflichtet gewesen, der Antragstellerin zu jeder beanstandeten Rechtsverletzung mitzuteilen, wer Veranlasser des Uploads ist. Der Antragstellerin obläge es demgemäß bei dem Entdecken neuer Rechtsverstöße, zumindest konkret nachfragen, ob diese auf einen der bekannten Rechtsverletzer zurückgehen. Diese Frage wäre von den Antragsgegnern zu beantworten. Die jeweils gegebenen Informationen hätten dabei möglicherweise nicht vollständig, aber zumindest so eindeutig sein, dass die Antragstellerin bei wiederholten Verstößen zweifelsfrei erkennen könnte, ob es sich um denselben Nutzer (bzw. dieselbe IP-Adresse) handelt und deshalb nunmehr eine aktive Prüfungspflicht der Antragsgegner besteht.

f. Derartige Informationen haben die Antragsgegner in der Vergangenheit jedoch nur äußerst gelegentlich an die Antragstellerin weitergegeben. Diese hat in der beigezogenen Parallelsache 5 U 119/07 ausdrücklich vorgetragen, dass sie von dem Antragsgegner zu 2. lediglich die IP-Adressen der beiden Vertreiber von Raubkopien genannt bekommen hat, die in M. (...) bzw. in T. (...) sitzen. Die Antragsgegner haben sich indes in der Vergangenheit nur anfangs kooperativ gezeigt. Die Antragstellerin hat in jener Akte weiter ausgeführt, dass der dortige Antragsgegner "nicht einmal die ganz am Anfang der Auseinandersetzung noch offen gelegten IP-Adressen" mehr preis geben mag, sondern sich weigert, "auch nur die geringsten Informationen über die Verletzer zu geben." Für den vorliegenden Fall gilt nichts anderes. Vor diesem Hintergrund waren es die Antragsgegner selbst, die die Antragstellerin unter Verstoß gegen die ihnen obliegenden Mitwirkungshandlungen außer Stande gesetzt haben, zumindest im Hinblick auf konkrete Verstöße einzelner Nutzer eine Wiederholungsgefahr darlegen zu können.

g. Der Senat hat aus Anlass des vorliegenden Rechtsstreits nicht darüber zu entscheiden, ob die Antragsgegner aus anderen Gründen eine Rechtspflicht treffen kann, nicht nur den ? zur Vermeidung erneuter Rechtsverletzungen ausreichenden ? elektronischen Ursprungsort, sondern darüber hinaus die persönliche Identität ihrer Nutzer festzustellen, insbesondere derer, die rechtsverletzende Handlungen begehen. Eine derartige Verpflichtung des Betreibers eines Meinungsforums hat etwa das OLG Düsseldorf unter Zumutbarkeitsgesichtspunkten selbst im Bereich der Bekämpfung von Kinderpornographie ausdrücklich abgelehnt (OLG Düsseldorf MMR 06, 553, 555). Aus diesen Gründen muss sich der Senat auch nicht im Einzelnen mit den Argumenten der Parteien zu den Möglichkeiten einer Manipulation von Identitätsangaben bzw. von Identitätsdiebstählen befassen. Denn vorliegend geht es allein um eine Unterlassungsverpflichtung der Antragsgegner und nicht um die Frage, ob bzw. welchem Umfang diese verpflichtet sind, Rechtsinhabern wie der Antragstellerin Auskünfte zu erteilen bzw. an der Aufklärung von Rechtsverletzungen mitzuwirken. Das Verlangen der Antragstellerin, die Antragsgegner müssten zur Verhinderung künftiger Rechtsverletzungen alle ihre Nutzer in einer Weise registrieren, dass diese eindeutig ? und zwar nicht nur über eine IP-Adresse, sondern als natürliche Person ? identifizierbar seien, könnte ersichtlich zu unzumutbaren Belastungen der Antragsgegner führen. Eine derartige Maßnahme würde in der Tat das gesamte Geschäftsmodell ihres Dienstes in Frage stellen. Zwar mag es sinnvoll sein, die Identität der Nutzer eines Internet-Dienstes zu kennen. Der Senat vermag allerdings nicht zu erkennen, dass dies eine zwingende Voraussetzung für ein zulässiges Geschäftsmodell ist. Gerade der Erfolg des Internets beruht zu einem ganz erheblichen Teil ? zulässigerweise ? auf dem Grundsatz der Anonymität, lässt man die "Spuren" außer Betracht, die jeder Nutzer zwangsläufig im Internet hinterlässt. Auch Dienste wie diejenige, die die Antragsgegner betreiben, müssen sich hierauf zulässigerweise einstellen dürfen, ohne dass ihnen der Vorwurf gemacht werden kann, schon deshalb sehenden Auges täterschaftlich und schuldhaft Rechtsverletzungen Vorschub zu leisten. Entscheidend bleibt vielmehr stets die Frage, ob es dem Betreiber des Dienstes ? auch ohne Kenntnis der handelnden natürlichen Person ? gelingt, nach dem Hinweis auf eine konkrete Rechtsverletzung weitere gleichartige Rechtsverletzungen aus derselben "Quelle" zu unterbinden.

h. Es ist für den Senat nicht ersichtlich, dass einer derartigen Informationspflicht unüberwindbare datenschutzrechtliche Bedenken entgegenstehen.

aa. Die Antragsgegner sind auf ihre datenschutzrechtlichen Ausführungen in der zweiten Instanz nicht mehr substantiiert zurückgekommen, so dass auch der Senat keine Veranlassung hat, sich aus Anlass dieses Rechtsstreits mit den komplexen datenschutzrechtlichen Fragen im Zusammenhang mit dem TMG näher zu befassen. Der vorliegende Rechtsstreit bietet dem Senat insbesondere keine Veranlassung, sich mit der in

der Rechtsprechung zum Teil kontrovers erörterten Frage (siehe z. B. AG Berlin CR 08, 194) zu befassen, ob bzw. unter welchen Voraussetzungen IP-Adressen von Nutzern gespeichert oder gar herausgegeben werden dürfen.

aaa. Die Antragsgegner haben sich in der Senatsverhandlung insoweit darauf berufen, dass ihnen hierbei möglicherweise ein Verstoß gegen das Fernmeldegeheimnis zur Last gelegt werden könnte. Dieser Umstand entlastet sie indes nicht. Sollte diese Auffassung der Antragsgegner richtig bzw. in rechtlicher Hinsicht vorzugswürdig sein, hätte dies zwangsläufig zur Folge, dass die Antragsgegner außer Stande sind, nach Maßgabe der von dem Bundesgerichtshof in den Entscheidungen "Internet-Versteigerung II" sowie "Jugendgefährdende Medien bei X" aufgestellten Grundsätze dem Rechtsinhaber die Verfolgung z. B. von Urheberrechtsverstößen zu ermöglichen. Denn diese Grundsätze setzen in der Regel voraus, dass der Rechtsinhaber zum Nachweis der Wiederholungsgefahr ? wie ausgeführt ? darlegen kann, dass Rechtsverstöße erneut aus derselben Quelle entspringen. Hierfür ist zumindest eine eindeutig zuzuordnende IP-Adresse erforderlich.

bbb. Sofern die Antragsgegner datenschutzrechtlich tatsächlich außer Stande sein sollten, dem Rechtsinhaber diese Art des Nachweises einer Rechtsverletzung zu ermöglichen, die zumindest ? auch ohne Kenntnis weiterer personenbezogener Daten des Nutzer ? zu einer Sperrung der konkreten IP-Adresse führen kann, stellt sich schon deshalb das gesamte Geschäftsmodell der Antragsgegner unter der Internetadresse www...com als rechtlich nicht schützenswert dar. Die Antragsgegner haben zu dem Dienst www...com ausgeführt, dass bei diesem Dienst täglich ca. 150.000 Dateien neu eingestellt werden. Nach den Angaben der Antragsgegner in der Senatsverhandlung liegt der Anteil der Dateien mit urheberrechtsverletzender Software bzw. Raubkopien bei "RapidShare" bei 5 bis 6% der gespeicherten Dateien. Bei einem täglichen Volumen von 150.000 neu eingestellten Dateien bedeutet dies, dass selbst nach den eigenen Angaben der Antragsgegner jeden Tag (!) ca. 9.000 Dateien mit rechtsverletzender Software neu in ihren Dienst eingestellt werden. Bei dem Dienst www...com sind nach den Angaben der Antragsgegner ca. 28 Mio. Dateien gespeichert. Dies bedeutet ? ebenfalls nach den Angaben der Antragsgegner ? einen Anteil rechtsverletzender Dateien in Höhe von ca. 1,68 Mio. Dateien. Wenn sich die Antragsgegner vor diesem Hintergrund ? zu Recht oder zu Unrecht ? auf den Standpunkt stellen, eine Rückverfolgung des Uploads urheberrechtswidriger Software bzw. eine Kooperation mit Rechteinhabern wie der Antragstellerin sei ihnen aus Rechtsgründen nicht möglich, so belegt dieser Umstand mit aller Deutlichkeit, dass das Geschäftsmodell der Antragsgegner schon aus diesem Grunde nicht den Schutz der Rechtsordnung verdient. Denn keine Rechtsordnung kann hinnehmen, dass tagtäglich allein über eine einzige Internetseite sehenden Auges Rechtsverletzungen in diesem Umfang begangen werden,

ohne dass dem Rechtsinhaber eine Möglichkeit zur Seite steht, in Abstimmung mit dem Betreiber des Dienstes zumindest den Nachweis zu führen, dass wiederholte Rechtsverletzungen aus derselben Quelle stammen und diese deshalb von der weiteren Nutzung des Dienstes wirksam ausgeschlossen werden muss.

bb. Die Antragsgegner sind auch nicht rechtlich verpflichtet, ihren Dienst ohne vorherige Registrierung und Erfassung ihrer Nutzer unter Wahrung der Anonymität zur Verfügung zu stellen. Gemäß § 12 Abs. 1 TMG dürfen personenbezogene Daten nur nach Maßgabe dieses Gesetzes erhoben werden. Gemäß § 13 Abs. 6 TMG gilt: "Der Diensteanbieter hat die Nutzung von Telemedien und ihre Bezahlung anonym oder unter Pseudonym zu ermöglichen, soweit dies technisch möglich und zumutbar ist. Der Nutzer ist über diese Möglichkeit zu informieren." Eben an dieser Zumutbarkeit fehlt es hier, wie noch auszuführen sein wird.

12. Sofern die Antragsgegner derartige Möglichkeiten der notwendigen Registrierung, d. h. einer datenschutzrechtlich zulässigen Identifikationsfeststellung bzw. Zugangsbeschränkung ergreifen würden, stünden ihnen auch wirkungsvolle Möglichkeiten zur Verfügung, künftige Urheberrechtsverletzungen entweder vollständig zu unterbinden oder zumindest mit der erforderlichen Gewissheit feststellen zu können, in welchen Fällen "Wiederholungstäter" ihren Dienst rechtsmissbräuchlich nutzen, um damit den Rechteinhabern eine Grundlage verschaffen zu können, gegen Rechtsverletzungen vorzugehen.

c. Im Rahmen des sich hieraus ergebenden konkreten Prüfungsumfangs ist den Antragsgegnern eine wirkungsvolle Verhinderung künftiger Rechtsverletzungen auch möglich und zumutbar.

aa. Jedenfalls bei einem Upload potenziell rechtsverletzender Software durch die bereits insoweit als Rechtsverletzer in Erscheinung getretenen Nutzer mussten die Antragsgegner nunmehr die Dateien inhaltlich konkret und umfassend z. B. über unverwechselbare Suchbegriffe nach Hinweisen auf Rechtsverletzungen durchsuchen. Hierbei können sich die Antragsgegner in der Regel auf solche Dateien beschränken, die von ihrer Art und Struktur überhaupt als rechtsverletzend in Betracht kommen. Insoweit mag es ? dies kann der Senat nicht abschließend überblicken ? bestimmte Dateitypen (z. B. *.mp3-Dateien) geben, die jedenfalls kein Indiz für eine Rechtsverletzung zulasten gerade der Antragstellerin bieten, mögen diese auch zulasten anderer Urheber (insbesondere Anbietern von urheberrechtlich geschützten Musikwerken) potenziell rechtsverletzend sein.

bb. Soweit die Antragsgegner in dem beigezogenen Parallelrechtsstreit 5 U 119/07

bestreiten, dass eine derartige inhaltliche Überprüfung erfolgreich vorgenommen werden könne, bleibt ihr Vorbringen ohne Überzeugungskraft. Eine Suche ist in jedem Fall nach dem Produktnamen sowie dem Hersteller/Urheberrechtsberechtigten bzw. einer Kombination aus beiden Suchbegriffen möglich und im Regelfall erfolgversprechend. Hierzu bedarf es keiner komplexen Suchfunktionen. Soweit Dateien aufgeteilt und erst später vom Nutzer wieder zusammengesetzt werden sollen, ist hinzunehmen, dass einzelne Dateipakete möglicherweise keinen Anlass bieten, eine Urheberrechtsverletzung der zu überprüfenden Art zu vermuten. Ausreichend kann es in diesen Fällen möglicherweise sein, dasjenige Datenpaket zu blockieren bzw. zu löschen, in dem sich die Hinweise auf eine Urheberrechtsverletzung befinden. Sofern die Antragsgegner trotz derartiger Überprüfungen keine Hinweise auf eine Rechtsverletzung zu finden vermögen, obwohl es sich tatsächlich um eine rechtsverletzende Software handelt, kann ihnen gegebenenfalls ? ohne dass der Senat über die insoweit anzulegenden Kriterien vorliegend zu entscheiden hat ? nicht der Vorwurf der Verletzung von Prüfungspflichten gemacht werden. Wann eine solche Situation gegeben ist, lässt sich letztlich erst anhand des konkreten Einzelfalls im Rahmen eines Ordnungsmittelverfahrens beurteilen. Dies mag etwa ? wie die Antragsgegner in dem Rechtsstreit 5 U 119/07 behaupten ? dann der Fall sein, wenn zum Auffinden der Hinweise auf den Programmnamen bzw. den Urheberrechtsberechtigten erst bestimmte Installationsroutinen durchlaufen werden müssen. In diesem Umfang ist es notwendig ? und zulässig ? die Beurteilung einer Rechtsverletzung in gewissem Maße von dem Erkenntnisverfahren in das Vollstreckungsverfahren zu verlagern. Eine umfassende, jeden Einzelfall trennscharf abgrenzende allgemeine Verbotsfassung wird in diesen Fällen letztlich nicht zu erreichen sein. Dies ändert indes nichts daran, dass die Antragsgegner rechtlich verpflichtet sind, umfassende Prüfungsmaßnahmen vorzunehmen.

d. Soweit die Antragsgegner ? insbesondere in dem beigezogenen Parallelverfahren 5 U 119/07 ? die Problematik ansprechen, dass eine Aufspaltung eines urheberrechtsverletzenden Produkts in mehrere Einzeldateien auch von intelligenten Filtermechanismen nicht erkannt bzw. nachvollzogen werden kann, mag diese Schwierigkeit zutreffend sein. Das Problem stellt sich indes jedenfalls dann nicht, wenn ? wie dies der Regelfall ist ? alle Einzelteile von demselben Nutzer hoch geladen werden. In diesem Fall können die Antragsgegner die gebotene Querverbindung herstellen. Wenn die Einzeldateien durch unterschiedliche Nutzer hoch geladen werden, von denen z. B. einzelne noch nicht als Rechtsverletzer aufgefallen sind, besteht insoweit möglicherweise auch keine Handlungspflicht der Antragsgegner. In diesen Fällen ist die Gefahr einer Rechtsverletzung aber auch ausgesprochen gering, weil die Software in der Regel nur bei einer vollständigen Installation sämtlicher Einzeldateien lauffähig ist. Wenn auch nur eine dieser Dateien die Filtersoftware nicht passiert, weil sie verdächtige Bestandteile enthält, kann das Gesamtprogramm im Zweifel nicht mehr erfolgreich installiert werden, weil

Installationsprogramme in der Regel die Integrität und Vollständigkeit der erforderlichen Dateien überprüfen. Dementsprechend können derartige Fälle als praxisfern vernachlässigt werden.

e. Sofern von derart "verdächtigen" Nutzern gepackte Dateien hochgeladen werden, haben die Antragsgegner diese Dateien vor der Einstellung in ihren Dienst zu entpacken, weil anders die gebotene umfassend inhaltliche Kontrolle im Zweifel nicht gewährleistet werden kann. Soweit derartige gepackte Dateien verschlüsselt oder mit einem Passwortschutz hochgeladen werden, müssen die Antragsgegner den Upload wirksam (aber möglicherweise gleichwohl automatisiert) zurückweisen, wenn sie sich nicht dem Vorwurf eines schuldhaften Verstoßes gegen ihrer Unterlassungsverpflichtung aussetzen wollen.

f. Das Risiko, dass rechtsuntreue Nutzer einer derartigen Erfassung in Zukunft auszuweichen versuchen, sobald diese bekannt wird, liegt allerdings ebenfalls erkennbar auf der Hand. Die Möglichkeiten hierzu sind vielfältig und reichen von Registrierungen unter neuen Identitäten/E-Mail-Adressen bis zu ständig wechselnden IP-Adressen. Die Antragsgegner sind grundsätzlich nicht verpflichtet, alle ihre Nutzer unter einen Generalverdacht zu stellen. Sie dürfen sich deshalb im Prinzip auf bislang bekannte Rechtsverletzer beschränken. Insbesondere sind sie nicht notwendigerweise gehalten, weitere ? zu eindeutiger Identifikation geeignete ? personenbezogene Nutzerdaten in jedem Einzelfall zu erheben. Allerdings sind die Antragsgegner auf der anderen Seite rechtlich zwingend verpflichtet, sich nach den ihnen im Rahmen eines rechtlich zulässigen Geschäftsmodells ? dazu noch im Folgenden ? zur Verfügung stehenden Möglichkeiten verlässliche Kenntnis von rechtsverletzenden Quellen bzw. Nutzern zu verschaffen, um diese von der weiteren Inanspruchnahme ihres Dienstes ausschließen zu können.

g. Diese ? im Umfang begrenzten ? inhaltlichen Prüfungsmaßnahmen sind den Antragsgegnern bei Abwägung mit den berechtigten Interessen der Antragstellerin nicht nur im Zeitaufwand, sondern auch wirtschaftlich und sicherheitstechnisch ohne weiteres zumutbar. Soweit die Antragsgegner für die Überprüfung entpackter Dateien zusätzliche Server anschaffen müssen, um diese Prüfungsmaßnahmen abgegrenzt von ihrem laufenden System vornehmen zu können, ist dieser Aufwand überschaubar und zur Aufrechterhaltung eines zulässigen Geschäftsmodells zumutbar. Die von den Antragsgegnern geschilderte Unmöglichkeit einer derartigen Maßnahme bezog sich allein auf die flächendeckende Überprüfung, um die es hier nicht geht. Auch die Sicherheitsbedenken der Antragsgegner können sie nicht von der Verpflichtung entbinden, zumindest Dateien von solchen Nutzern zu entpacken, die in der Vergangenheit bereits wegen Rechtsverletzungen zulasten der Antragstellerin aufgefallen sind. Es mag sein, dass hierbei durch Viren, Trojaner, Exploits, Aktivbomben usw. vielfältige Gefahren für die

Integrität der Systeme der Antragsgegner drohen. Jedenfalls im Hinblick auf die zahlenmäßig begrenzte Nutzergruppe, hinsichtlich derer überhaupt nur eine inhaltliche Prüfungspflicht besteht, müssen die Antragsgegner unter Abwägung der Interessen der Antragstellerin Mittel und Wege finden, um diese Risiken beherrschbar zu machen. Hierzu dürften sich ? was die Parteien bereits diskutiert haben ? gegeneinander abgegrenzte Systeme für den normalen Sharehosting-Betrieb und die inhaltliche Überprüfung verdächtiger Dateien anbieten. Sofern hiermit verbundene Investitionen den Antragsgegnern unverhältnismäßig erscheinen, bleibt die weitere Möglichkeit, gepackte und/oder verschlüsselte und/oder passwortgeschützte Dateien von bereits als rechtsverletzend in Erscheinung getretenen Nutzern (ebenso wie von denjenigen, die auf einen Verzicht der Nutzung einer dynamischen IP-Adresse bzw. einen Proxy-Server nicht bereit sind) generell abzuweisen. Hierdurch wird weder das Geschäftsmodell der Antragsgegner als solches in Frage gestellt noch werden berechnete Interessen rechtmäßiger Nutzer beeinträchtigt. Sofern die Antragsgegner trotz der damit verbundenen überproportional großen Risiken weiterer Rechtsverletzungen auch rechtsuntreuen Nutzern weiterhin das Hochladen gepackter Dateien gestatten wollen ? wozu sie unter keinem Gesichtspunkt verpflichtet sind -, müssen sie die damit einhergehenden erhöhten Aufwendungen im eigenen Interesse selbst tragen.

h. Mit diesen Maßnahmen werden insbesondere auch die Interessen rechtstreuer Nutzer nicht unangemessen beeinträchtigt. Es mag sein, dass gerade gegenüber diesen Nutzern ein pro-aktives Entpacken von Dateien bzw. Zurückweisen von verschlüsselten bzw. passwortgeschützten Dateien unzumutbar ist, weil derartige Nutzer ? wie die Prozessbevollmächtigten der Antragsgegner bei der Übermittlung vertraulicher anwaltlicher Schriftsätze ? ein berechtigtes Interesse daran haben, Dritten ? unter Anschluss der Antragsgegner ? Zugang zu und Kenntnis von ihren Dateien zu verweigern. Es ist indes als lebensfern auszuschließen, dass derartige ? rechtstreue ? Nutzer von dem erforderlichen Prüfungsraster der Antragsgegner, das ausschließlich bereits in Erscheinung getretene Urheberrechtsverletzer zulasten der Antragstellerin berücksichtigt, erfasst werden können. Ist dies gleichwohl der Fall, so stellt sich eine inhaltliche Prüfung jedenfalls nicht als unverhältnismäßig dar und ist von diesen (ansonsten rechtstreuen) Nutzern hinzunehmen.

i. Durch die beschriebenen Prüfungsmaßnahmen würde weder das Geschäftsmodell der Antragsgegner grundlegend in Frage gestellt noch würden diese unangemessen in ihrer geschäftlichen Tätigkeit behindert bzw. mit unzumutbaren Pflichten belegt. Rechtlichen Schutz verdient das Geschäftsmodell der Antragsgegner nur mit derjenigen Zweckausrichtung, wie sie von ihnen selbst vorgetragen worden ist. Die Antragsgegner haben erklärt, dass sie das Hochladen und Verteilen urheberrechtswidriger Software über ihre Dienste missbilligen. Soweit die Verhinderung künftiger Rechtsverletzungen durch

konkrete, im Einzelnen bekannte Nutzer, die in der Vergangenheit durch entsprechende Rechtsverletzungen bekannt geworden sind und deshalb auch für die Zukunft eine erhöhte Wahrscheinlichkeit gleichartiger Handlungen bieten, eine mit der wirksamen Überprüfung und Verhinderung notwendigerweise einhergehende Behinderung der Geschäftstätigkeit der Antragsgegner mit sich bringt, ist diese von ihnen hinzunehmen, weil sich hierin ein typisches Risiko ihres mit wirtschaftlicher Zielrichtung betriebenen Geschäftsmodells verwirklicht, aus dem die Antragsgegner Einkünfte erzielen. Soweit eine Prüfungspflicht besteht, schulden die Betreiber angemessene Bemühungen, entsprechende Angebote aufzudecken und zu entfernen. Sofern trotz angemessener Bemühungen ein vollständiger Ausschluss der fraglichen Angebote von dem Dienst technisch oder faktisch zuverlässig nicht möglich ist, fehlt es an einem Verstoß der Betreiber gegen die Prüfungspflicht (BGH WRP 07, 1173, 1179 ? Jugendgefährdende Medien bei X).

13. Einem Geschäftsmodell, welches derartige nahe liegende Identifikationsmöglichkeiten ungenutzt lässt, kann allerdings insgesamt die ernst zu nehmende Gefahr immanent sein, dass es für die (massenhafte) Begehung von Straftaten, Urheberrechtsverletzungen und unlauteren Wettbewerbshandlungen genutzt wird.

a. Eine solche Gefahr folgt insbesondere aus einer durch die Möglichkeit zur freien Wahl eines Pseudonyms gewährleisteten Anonymität, der Möglichkeit einer problemlosen Abwicklung im Fernabsatz sowie der für das Internet typischen, deutlich herabgesetzten Hemmschwelle potenzieller Nutzer, sich für entsprechende Angebote zu interessieren (BGH WRP 07, 1173, 1175 ? Jugendgefährdende Medien bei X). Ein solches Geschäftsmodell ist von der Rechtsordnung nicht gebilligt. Es verdient nicht den Schutz der Rechtsordnung. In diesem Fall kann sich der Betreiber auch nicht auf die Unzumutbarkeit der Erfüllung von Prüfungspflichten berufen, weil er seiner Unfähigkeit, diese zu erfüllen, durch sein Geschäftsmodell wissentlich und willentlich selbst Vorschub leistet. So verhält es sich auch im vorliegenden Fall im Bezug auf das Geschäftsmodell der Antragsgegner.

b. Tatsächlich lassen die Antragsgegner die unkontrollierte Nutzung ihres Systems in einem Umfang zu, welcher die vollständig anonyme Einstellung von Dateien ermöglicht, ohne dass im Nachhinein nachvollzogen werden kann, von welcher Person bzw. aus welcher Quelle diese stammen. Ein Geschäftsmodell, das auf derartigen Grundsätzen beruht, verdient nicht den Schutz der Rechtsordnung, weil es letztlich die berechtigten Interessen von Inhabern absoluter Sonderschutzrechte bewusst und sehenden Auges vollständig schutzlos stellt.

aa. Es ist ? und hierin liegt der wesentliche Unterschied in der Ausgangssituation zu den von dem BGH in Bezug auf den Internet-Marktplatz X aufgestellten Rechtsgrundsätzen ?

den Nutzern bei dem Geschäftsmodell der Antragsgegner schon jetzt praktisch uneingeschränkt möglich, ihre Identität vollständig zu verbergen.

aaa. Solange die Nutzer eine sog. "statische IP-Adresse" benutzen und sich direkt bei den Antragsgegnern anmelden, ist eine Identifikation zumindest über diese fest zugeordnete IP-Adresse möglich, deren Inhaber über den Anbieter der Telekommunikationsdienstleistung ermittelt werden könnte. Schon wenn die Benutzer einen sog. Proxy-Server verwenden, können die Antragsgegner nur die IP-Adresse dieses Servers erkennen, nicht jedoch diejenige Person, an die der Proxy-Server die Anfragen weiterleitet. Nicht weniger undurchschaubar gestaltet sich der Sachverhalt, wenn sich der Nutzer ? wie zumeist bei der Einwahl über einen Provider ? einer sog. "dynamischen IP-Adresse" bedient. In diesem Fall wird bei jeder Anfrage eine neue IP-Adresse zugeteilt, so dass es hierüber nicht möglich ist, frühere Rechtsverletzer eindeutig unmittelbar zu identifizieren und Wiederholungsfälle erkennbar zu machen. In allen diesen Möglichkeiten unterscheiden sich die Dienste der Antragsgegner von dem Internet-Marktplatz X. Denn dort ist in jedem Fall ein Nutzerkonto einzurichten und der Teilnehmer ist zumindest über seine "Alias-Bezeichnung" eindeutig identifizierbar. Diese lässt sich zwar theoretisch auch verändern bzw. gegen eine neue austauschen. Dies ist indes ungleich aufwändiger und komplizierter als das Verbergen bzw. der Wechsel der Identität im vorliegenden Fall. In jedem Fall kann X stets einen Nutzer von einem anderen unterscheiden und damit Wiederholungsfälle feststellen. Dies ist bei den Antragsgegnern letztlich nicht möglich, wenn der Nutzer ? was gerade bei den Rechtsverletzern der Fall sein wird ? seine Identität bewusst im Dunkeln halten will. Deshalb muss diesen Besonderheiten bei der Übertragung der von dem BGH in allen einschlägigen Entscheidungen in Bezug auf den Internetmarktplatz X entwickelten Grundsätze auf derartige "freie Plattformen" wie diejenigen der Antragsgegner Rechnung getragen werden.

bbb. Auf diese Besonderheiten hat die Antragstellerin im Rahmen des beigezogenen und zum Gegenstand des vorliegenden Rechtsstreits gemachten Parallelverfahrens 5 U 119/07 hingewiesen. Auch bestünden für die Antragsgegner zumutbare Lösungsmöglichkeiten. Sie wären zwar nicht notwendigerweise dazu verpflichtet, eine Registrierung durchzuführen. Sie könnten (und müssten) die Nutzung ihres Dienstes aber zumindest davon abhängig machen, dass der jeweilige Nutzer im Bedarfsfall über denjenigen Computer eindeutig zu identifizieren ist, über den er sich bei den Antragsgegnern angemeldet hat. Das bedeutet, dass die Antragsgegner eine Nutzung mit dynamischen IP-Adressen ausschließen und ihre Nutzer stattdessen verpflichten müssen, statische IP-Adressen ohne Zwischenschaltung eines Proxy-Servers zu verwenden. Nutzeranfragen die diesen Vorgaben nicht entsprechen, müssten die Antragsgegner notfalls zurückweisen. Tun sie dies nicht, sind sie für solche Rechtsverletzungen unmittelbar verantwortlich, die hiervon ausgehen. Alternativ

könnten die Antragsgegner u. U. möglicherweise auch weiterhin dynamische IP-Adressen bzw. eine Kontaktaufnahme über einen Proxy Server zulassen, wenn sich diese Nutzer freiwillig einem Registrierungsverfahren unterwerfen und dadurch ihre Identität jedenfalls im Verletzungsfall feststellbar gemacht haben.

ccc. Derartige Identifikationsmaßnahmen sind den Antragsgegnern zumutbar, und zwar selbst dann, wenn sie ihr Geschäftsmodell bedrohen und künftige Nutzer abschrecken. Denn das Geschäftsmodell der Antragsgegner verdient jedenfalls insoweit keinen rechtlichen Schutz, als es dazu geeignet ist, vielfältige Rechtsverletzungen im Internet unter dem Schutz völliger Anonymität und fehlender Nachvollziehbarkeit zu ermöglichen. Dass derartige Maßnahmen keinen vollständigen Schutz bieten, versteht sich von selbst. Gleichwohl können sie Rechtsverletzungen nachhaltig entgegenwirken (a. A. OLG Düsseldorf, a. a. O., das die Sperrung von IP-Adressen wegen bestehender Umgehungsmöglichkeiten für nicht zumutbar hält).

bb. Indes beschränken sich die Antragsgegner noch nicht einmal darauf, naheliegende Erkenntnis- bzw. Kontrollmöglichkeiten nicht zu nutzen. Vielmehr sind sie offensichtlich daran interessiert und bestrebt, jede Möglichkeit einer Identifizierung ihrer Nutzer aktiv zu verhindern. Aus dem Schriftsatz der Antragstellerin vom 21.02.08 in dem beigezogenen Parallelverfahren 5 U 119/07 ergeben sich eine Reihe handfester weiterer Indizien dafür, dass die Antragsgegner ? entgegen ihren nachhaltigen Beteuerungen ? tatsächlich keinerlei Interesse daran haben, an der Verhinderung bzw. Aufklärung von Rechtsverletzungen wie den von der Antragstellerin verfolgten mitzuwirken. Insbesondere dieser Umstand nimmt ihrem Geschäftsmodell die rechtliche Schutzfähigkeit.

aaa. Einem von der Antragstellerin eingereichten Artikel in der Zeitschrift "C. B. Spiele" (Anlage BB 3) ist ein Zitat des Geschäftsführers bzw. Verwaltungsrats der R. AG (B. C.) zu entnehmen, wonach die IP-Nummern der Free-User nach 24 Stunden gelöscht werden. Damit machen sich die Betreiber des Dienstes jede Auskunftsmöglichkeit und Nachvollziehbarkeit gezielt selbst unmöglich. Sie verwischen jede Spur, die zu dem Täter führen kann, sei diese auch noch so schwach. Da die Antragstellerin in der Regel innerhalb einer 24-Stunden-Frist von der Rechtsverletzung noch nicht einmal Kenntnis erlangt, kann sie auch über die Antragsgegner Wiederholungstäter nicht identifizieren. Soweit B. C. in der Senatssitzung erklärt hatte, seine diesbezügliche ? richtig wieder gegebene ? Darstellung sei unzutreffend, die Daten würden weiter gespeichert, entlastet dies die Antragsgegner nicht. Denn diese Äußerung zeigt einmal mehr, dass sich die Antragsgegner jedenfalls im Außenverhältnis den potentiellen Rechtsverletzern mit einer weitestgehenden Anonymität und fehlenden Nachverfolgbarkeit präsentieren.

bbb. Die Antragstellerin hatte mehrfach beanstandet, dass die Antragsgegner ihre geschäftlichen Aktivitäten bzw. ihre Server zum Teil in das Ausland verlagert und sich dadurch noch mehr dem inländischen Zugriff entzogen haben. Auch dieses Verhalten zeigt, dass die Antragsgegner offensichtlich bestrebt sind, einen Zugriff der inländischen Rechtsordnung auf ihren Dienst nicht zuzulassen bzw. zu erschweren.

(1) Während den Antragsgegnern unter Berücksichtigung der inländischen Nutzungsgewohnheiten ? insbesondere des Verbreitungsgrades von Heimcomputern und Internetanschlüssen in der Bundesrepublik Deutschland ? eine eingrenzende Identifizierung von Nutzern eher möglich ist, scheidet dies ? wie sogleich darzulegen ist ? bei ausländischen Geschäftsaktivitäten häufig aus. Die Verlagerung von Servern in das Ausland entzieht auch die darauf gespeicherten Nutzer- bzw. Verbindungsdaten möglicherweise weitgehend den stark ausdifferenzierten rechtlichen Regularien des Telekommunikationsrechts in Deutschland.

(2) Im Rahmen des beigezogenen Rechtsstreits 5 U 149/07 haben die Antragsgegner die besonderen Umstände der Zugangsgewohnheiten ihrer Nutzer dargelegt. Nach Angaben der Antragsgegner ist ihr kostenloser Dienst vor allem in "Entwicklungsländern" erfolgreich, in denen Internet-Nutzer nicht die hoch entwickelten Internet-Strukturen vorfinden, wie etwa in Deutschland (Anlage AG 1 zu 5 U 149/07). In derartigen Ländern ist das Internet nach der eigenen Aussage der Antragsgegner "weiten Teilen der Bevölkerung nur über Internet-Cafés zugänglich". Gerade vor diesem Hintergrund kann ? dies zeigt der eigene Vortrag der Antragsgegner ? der Versuch der Antragstellerin, zumindest über die Beanstandung von Wiederholungsfällen neue Rechtsverletzungen zu verhindern, nur dann erfolgreich sein, wenn die Antragsgegner bereit bzw. verpflichtet sind, in derartigen Fällen gegebenenfalls die jeweilige IP-Adresse, von der der Upload erfolgt ist, für die Zukunft vollständig zu sperren, und zwar in Kenntnis der Tatsache, dass dieser von einer Vielzahl wechselnder Benutzer in Anspruch genommen wird. Ein derartiges Vorgehen wäre selbst unter dem Gedanken des Diskriminierungsverbotes möglich und zulässig. Denn auch ein gewerblicher Anbieter muss derartige Sanktionen in Kauf nehmen, wenn aus seinem Einflussbereich heraus Rechtsverletzungen begangen werden.

(3) Problematisch ist hierbei darüber hinaus, dass bei dem Dienst www...com nach der ? unbestritten gebliebenen ? Darstellung der Antragstellerin in dem beigezogenen Parallelverfahren nunmehr selbst im Rahmen sog. "Premium-Accounts" für Nutzer aus dem Ausland ein Netzwerk ausländischer Zwischenhändler, sog. "Reseller", zwischengeschaltet worden sind. Diese erwerben Premium-Accounts zum Weiterverkauf an Endnutzer. Der Zahlungsverkehr zwischen dem Betreiber des Dienstes wird damit ausschließlich über die Reseller abgewickelt. Die Endnutzer erwerben eine Art "Prepaid-Card", mit der sie zu einem

bestimmten Festpreis befugt sind, die Dienste von www...com in Anspruch zu nehmen. Mit diesem Modell fehlt auch die letzte ? vom den Antragsgegnern gerade im Rahmen des "Premium-Accounts" nachhaltig betonte ? Möglichkeit der Identifizierung der Endnutzer über die Zahlungssysteme. Dem Betreiber des Dienstes ist nur der Reseller sowie das Volumen der ihm abgerechneten Accounts bekannt. Da diese Accounts im Ausland gegenüber dem Reseller auch durch Barzahlung, Webmoney und andere anonyme Zahlungssysteme abgewickelt werden können (Anlage BB 5 und BB 6 in dem Rechtsstreit 5 U 119/07), ist jegliche ? selbst theoretische ? Rückverfolgung der Endbenutzer ausgeschlossen. Die Antragstellerin weist zu Recht darauf hin, dass dieses System mit Resellern von www...com gerade in Ländern wie Russland, China, Iran, Pakistan, Marokko oder der Türkei, und damit in solchen Ländern angeboten wird, in denen die Herstellung von Raubkopien unterschiedlichster Produkte an der Tagesordnung ist. Ob die Antragsgegner ? wie die Antragstellerin meint ? damit gezielt auch die sich nach der deutschen Gesetzeslage ergebende Speicherpflicht und 6-monatige Aufbewahrungszeit für Verbindungsdaten (§ 113 a Abs. 1 und Abs. 4 Nr. 2 TKG) umgehen zu versuchen, bedarf im vorliegenden Rechtsstreit keiner Entscheidung.

ccc. Dieses gesamte Verhalten zeigt deutlich die mangelnde Bereitschaft der Verantwortlichen des Modells "RapidShare", eine Aufklärung von Rechtsverstößen durch ihre Tätigkeit auch nur zu ermöglichen bzw. gar hieran mitzuwirken. Damit stellt sich nach der Beurteilung durch den Senat die Feststellung als unausweichlich dar, dass das gesamte Geschäftsmodell der Antragsgegner von der Rechtsordnung nicht gebilligt wird und damit nicht schutzwürdig ist, weil es letztlich auf die massenhafte Begehung von Urheberrechtsverletzungen ausgerichtet ist bzw. die berechtigten Interessen der Urheberrechtshaber trotz bestehender zumutbarer Kontrollmechanismen in einer Weise schutzlos stellt, die in rechtlicher Hinsicht auch vor dem Hintergrund nur eingeschränkter Prüfungspflichten von Providern nicht akzeptabel ist.

c. Da die Antragsgegner in Kenntnis der begangenen Urheberrechtsverletzungen weiterhin einschränkungslos eine anonyme Nutzung ihres Dienstes zulassen, schneiden sie der Antragstellerin letztlich sehenden Auges den erforderlichen Nachweis wiederholter Begehungshandlungen ab, welchen diese benötigt, um ihre Rechte erfolgreich durchsetzen zu können. Denn ein Unterlassungsanspruch, mit dem das künftige Hochladen urheberrechtsverletzender Software unterbunden werden soll, setzt Wiederholungs- oder Erstbegehungsfahr voraus. Für die Annahme von Wiederholungsfahr ist eine vollendete Verletzung nach Begründung der Prüfungspflicht erforderlich (BGH WRP 07, 1173, 1179 ? Jugendgefährdende Medien bei X). Eine derartige Verletzung liegt vor, wenn ein Anbieter, der dem Betreiber bereits in der Vergangenheit wegen eines derartigen Verstoßes bekannt geworden ist, nachfolgend erneut gleichartige Angebote anbietet, sofern

der Betreiber insoweit nach den dargelegten Grundsätzen zu Prüfung verpflichtet war (BGH WRP 07, 1173, 1179 ? Jugendgefährdende Medien bei X). Hierzu kann und konnte die Antragstellerin aufgrund des Verhaltens der Antragsgegner keine substantiierten Angaben machen. Sie konnte insbesondere nicht konkret darlegen, dass von denselben Nutzern bzw. IP-Adressen, zu denen sie den Antragsgegnern für ihren jeweiligen Dienst konkrete Beanstandungen für die in diesem Rechtsstreit streitgegenständlichen Softwareprodukte mitgeteilt hatte, erneut gleiche Softwareprodukte rechtsverletzend hochgeladen worden sind. Nur in diesem Fall läge aufgrund der Besonderheiten der vorliegenden Fallgestaltung eine auf den Einzelfall bezogene Urheberrechtsverletzung vor. Indem die Antragsgegner der Rechtsinhaber derartige Nachweismöglichkeit abschneiden, nehmen sie ihrem eigenen Geschäftsmodell die rechtliche Schutzwürdigkeit.

d. Im Falle eines von der Rechtsordnung wegen der im Schutze der Anonymität massenhaft sanktionslos begehbaren (Schutz)Rechtsverletzungen nicht gebilligten Geschäftsmodells erweisen sich damit die ansonsten einschlägigen Kategorien einer "Wiederholungsgefahr" bzw. einer "Erstbegehungsgefahr" bereits strukturell als ungeeignet und können deshalb aus den genannten Gründen nicht als Voraussetzungen für das Einsetzen konkreter Prüfungspflichten verlangt werden. In Betracht kommt letztlich nur eine einschränkungslose Prüfungspflicht, nachdem die Antragsgegner auf einen konkreten Erstverstoß (irgend)eines ihrer Nutzer in Bezug auf den Streitgegenstand hingewiesen worden sind.

14. Vor diesem Hintergrund muss es von den Antragsgegnern als zwangsläufige Folge hingenommen werden, dass sie auch legale Programmkopien für ihre Nutzer nicht mehr speichern dürfen.

a. Allerdings ist es nie vollkommen auszuschließen, dass auch ein bisher rechtsuntreuer Nutzer von Software der Antragstellerin zu einem späteren Zeitpunkt in rechtstreuer Weise eine derartige Software über die Dienste der Antragsgegner hoch zu laden versucht (bzw. dies behauptet). Derartige Nutzungsgewohnheiten liegen allerdings deutlich außerhalb der üblichen Lebenswahrscheinlichkeit. In derartigen Fällen wäre es notwendig, dass die Antragsgegner von dem Nutzer gegebenenfalls einen Nachweis seiner Rechtsinhaberschaft und des Zwecks des Uploads verlangen, wenn er den Dienst hierfür in Anspruch nehmen will. Ein derartiges Verhalten ist auch sowohl dem Nutzer als auch den Antragsgegnern zumutbar, weil anders in derart besonders gelagerten Einzelfällen ein rechtswidriges nicht verlässlich von einem rechtmäßigen Verhalten unterschieden werden kann. Ein unzumutbarer Arbeitsaufwand ist hiermit ebenfalls nicht verbunden, weil sich derartige Fallgestaltungen auf Ausnahmesituationen beschränken werden.

b. Wenn die Antragsgegner der Antragstellerin die Verfolgung von rechtswidrigen erstellten

Programmkopien unmöglich machen, ist auch dieser eine Differenzierung nach rechtswidriger/rechtmäßigen Programmen unmöglich, so dass nur ein vollständiges Verbot in Betracht kommen kann. Deshalb muss der Senat auch dem Einwand der Antragsgegner, sie könnten nicht unterscheiden, ob es sich bei eingestellten Programmen nicht möglicherweise um legale Sicherungskopien gem. § 69 d Abs. 2 UrhG handelt, nicht näher nachgehen. Allerdings dürfte bereits der Umstand, dass derartige Dateien auf einen Server hoch geladen werden, die Möglichkeit ausschließen, dass es sich hierbei um legale Sicherungskopien handelt. Denn insoweit ist eine Verbreitung über einen externen Server unzulässig. Die Antragstellerin weist zutreffend darauf hin, dass hiergegen auch der von den Antragsgegnern auf der Eingangsseite ihres Dienstes angebrachte Aufruf "Download-Link verteilen" spricht.

c. Vor diesem Hintergrund stellt sich auch der Verfügungsantrag nicht deshalb als zu weit dar, weil den Antragsgegnern jedwede Handlungen in Bezug auf die streitgegenständliche Software untersagt werden. Der Antrag sowie der Tenor beschränken sich nicht auf Raubkopien, sondern erfasst auch legale Software, die ordnungsgemäß erworben und von der Klägerin autorisiert ist. In diesem Zusammenhang sind allerdings Verwertungsformen denkbar, die möglicherweise von dem Verbot nicht erfasst werden sollen. Denkbar ist z. B., dass ein berechtigter Nutzer sein Softwareprogramm per Internet über die Dienste der Antragsgegner von seinem Hauptwohnsitz in H. zu seiner Ferienwohnung auf S. unkörperlich zu übertragen versucht, um es dort künftig (ausschließlich) zu nutzen, nachdem er es auf seinem heimischen Computer deinstalliert hat. Denkbar ist weiterhin, dass ein berechtigter Nutzer die Lizenz für sein Softwareprogramm an einen Dritten verkauft und diesem die hierzu gehörende ? legale ? Software körperlos über den Dienst der Antragsgegner zur Verfügung stellt. Die Tatsache, dass damit möglicherweise auch Sachverhalte erfasst werden, in denen die Antragstellerin ihren Nutzern z. B. bestimmte Nutzungsformen (z. B. Nutzung auf zwei Rechnern, sofern dies nicht gleichzeitig geschieht) vertraglich einräumt, ist Folge der von den Antragsgegnern selbst angelegten vollständigen Anonymität und Intransparenz ihres Systems und deshalb von diesen hinzunehmen.

d. Deshalb kommt die von den Antragsgegnern in dem Parallelrechtsstreit 5 U 149/07 geforderte Beschränkung/Klarstellung des Unterlassungstenors dahingehend, dass eine Unterlassungspflicht dann nicht bestehe, wenn es zwar zu Rechtsverstößen kommt, diese von ihnen aber auch bei dem Einsatz zumutbarer Überprüfungsmaßnahmen nicht habe verhindert werden können, im vorliegenden Fall gerade nicht in Betracht.

15. Mit dem angegriffenen Verhalten sind die Antragsgegner ? neben ihrer Verantwortung wegen einer Vervielfältigung aus § 16 UrhG ? als Störer einer Urheberrechtsverletzung auch gemäß § 19a UrhG in der Form des "öffentlich zugänglich Machens" bzw. "öffentlich

zugänglichlich machen zu lassen" rechtsverletzender Software zur Unterlassung verpflichtet.

a. Allerdings lehnt das OLG Köln (a. a. O., S. 42) ein täterschaftliche Handeln durch Sharehosting-Provider durch öffentliches Zugänglichmachen ausdrücklich mit der Begründung ab, dies geschehe nur durch den Nutzer. Auch andere Stimmen in der Literatur (Sieber/Höfingher MMR 04, 575, 579) stehen auf dem (im Einzelnen allerdings streitigen) Standpunkt, der Hostprovider verletze als technischer Dienstleister mangels Kenntnis des konkreten Inhalts nicht das Recht der öffentlichen Zugänglichmachung im Sinne von § 19a UrhG. Der Senat hat keine Veranlassung, zu diesen Meinungsunterschieden im vorliegenden Fall Stellung zu nehmen. Denn Grundlage der Verantwortlichkeit der Beklagten ist im vorliegenden Fall eine Störerhaftung. Für diese Haftung ist es ohne Bedeutung, ob die Antragsgegner selbst täterschaftlich handeln. Ein täterschaftliches Handeln durch ihre Nutzer reicht aus. Dies liegt unzweifelhaft vor.

b. Die Antragsgegner wenden zu Unrecht ein, die streitgegenständlichen Softwareprogramme der Antragstellerin würden in ihren Diensten nicht "öffentlich zugänglich gemacht" i. S. v. § 19a UrhG. Diese rechtliche Sichtweise wird den Besonderheiten des Dienstes der Antragsgegner nicht gerecht.

aa. Zwar trifft es zu, dass für den Bereich der legalen Nutzung des Dienstes der Antragsgegner eine Bekanntgabe des Speicherortes der hochgeladenen Dateien in der Regel nur gegenüber einzelnen berechtigten Nutzer, nicht jedoch gegenüber der Öffentlichkeit erfolgt.

bb. Anders verhält sich die Sachlage aber bei der illegalen Nutzung durch das Hochladen von Raubkopien, um die es im vorliegenden Rechtsstreit geht. Hierbei erfolgt das Hochladen der Dateien ausdrücklich zu dem Zweck, dass eine Vielzahl ? in der Regel unbekannte Nutzer ? diese Dateien sich herunterladen und nutzen können. Zu diesem Zweck werden ? dies ist zwischen den Parteien nicht streitig ? die Speicheradressen als links auf eine Vielzahl von "Raubkopierer"-Websites bekannt gemacht. Die Eröffnung der Nutzung der Raubkopien durch unterschiedliche Personen über diese Websites, die damit den Zugriff auf die richtige Speicheradresse im Dienst der Antragsgegner ermöglichen, erfolgt erklärtermaßen mit dem Zweck der öffentlichen Zugänglichmachung der Raubkopien. Damit werden diese zugleich auch auf den Diensten www...de und www...com der Antragsgegner öffentlich zugänglich gemacht, selbst wenn der interessierte Nutzer ohne Kenntnis der konkreten Speicheradresse die Dateien in diesen Diensten nicht finden kann.

c. Die Antragsgegner verwirklichen daneben auch die Handlungsalternative des "öffentlich zugänglich machen zu lassen". Der Senat kann dahinstehen lassen, ob bereits eine dieser Handlungsformen grundsätzlich geeignet wäre, das Charakteristische des Verstoßes zu erfassen. Denn jedenfalls sind Handlungsformen denkbar, in denen nebeneinander sowohl die eine als auch die andere Handlungsformen verwirklicht sein kann. Dies ist insbesondere dann der Fall, wenn die Antragsgegner ihre geschäftlichen Aktivitäten (einschließlich der erforderlichen Serverkapazitäten) zum Teile selbst betreiben und im Übrigen durch einen eingeschalteten Dienstleister für sich betreiben lassen. In diesem Fall ist es ? je nach Ausgestaltung des Geschäftsmodells ? vorstellbar, dass das "öffentliche zugänglich machen" nicht durch die Antragsgegner selbst, sondern durch die von ihnen eingeschalteten Personen erfolgt. In diesem Falle wäre den Antragsgegner gleichwohl vorzuwerfen, dass sie das streitgegenständliche Schutzobjekt durch Dritte "öffentlich zugänglich machen lassen".

16. Markenrechtliche Ansprüche aus § 14 Abs. 2 Nr. 2 beziehungsweise Nr. 3 MarkenG an der Bezeichnung "IBM" und den weiteren für die Antragstellerin geschützten Marken stehen der Antragstellerin demgegenüber auf der Grundlage des hier zur Entscheidung stehenden Sachverhalts nicht zu, so dass der Verfügungsantrag zu Ziff. 2 abzuweisen ist.

a. Dabei kann der Senat dahinstehen lassen, ob die Antragsgegner im geschäftlichen Verkehr handeln und ob die von der Antragstellerin verfolgten Antragsalternativen geeignet sind, das Charakteristische des rechtsverletzenden Handelns der Antragsgegner hinreichend zu erfassen.

b. Denn jedenfalls fehlt es vorliegend an einer markenmäßigen Verwendung der Kennzeichnungen durch die Antragsgegner sowie deren Nutzer in demjenigen Handlungsumfelds auf den Servern des Dienstes www...com, für den die Antragsgegner verantwortlich sind.

aa. An einer kennzeichenmäßigen Verwendung der Marken der Antragstellerin durch die rechtsverletzenden Nutzer der Antragsgegner bei der Verwendung der installierten Programme vor dem Einstellen von Raubkopien in die Dienste bzw. nach dem Installieren der heruntergeladenen Raubkopien aus den Diensten der Antragsgegner kann kein Zweifel bestehen. Denn die in den installierten Dateien erscheinenden Marken und sonstigen Bezeichnungen sollen erkennbar die Zugehörigkeit der jeweiligen Programme zu dem Geschäftsbetrieb der Antragstellerin dokumentieren. Darum geht es vorliegend jedoch nicht. Denn diese Handlungsalternativen liegen außerhalb der den Antragsgegnern konkret zuzurechnenden Handlungsformen.

bb. Bei dem Hochladen, während des Speicherns und bei dem Herunterladen der rechtsverletzenden Dateien besteht in markenrechtlicher Hinsicht indes die Besonderheit, dass die in den einzelnen Dateien enthaltenen Marken ohne eine Installation des gesamten Programms als solche nicht sichtbar sind. Eine derartige Installation wird jedenfalls nicht im Rahmen der Dienste der Antragsgegner, sondern erst später ? unabhängig davon ? auf dem jeweiligen PC des Nutzers vorgenommen. Eine Marke kann indes nur dann ihre Hauptfunktion als Herstellerhinweis erfüllen, wenn sie für den Nutzer sichtbar, erkennbar oder zumindest auffindbar ist. Dieses Merkmal ist im vorliegenden Fall nicht erfüllt.

cc. Der Umstand, dass der Textstring "IBM" (oder die aus dem Verfügungsantrag ersichtlichen Produktbezeichnungen) mehrfach in den Programmen enthalten ist, reicht für eine Markenverletzung nicht aus. Insofern liegt eine abweichende Situation als bei Metatags vor. Bei diesen ist es ihre Zweckbestimmung, von Suchmaschinen als Marke bzw. Bestimmungshinweis erkannt ? und entsprechend behandelt ? zu werden, obwohl sie nicht offen zu Tage treten. Damit wird die Hauptfunktion der Marke in einer dem elektronischen Geschäftsverkehr typischen Weise verwirklicht. Dies ist hier nicht der Fall. Die in den raubkopierten Programmen enthaltenen Marken sollen vielmehr bis zur Installation des Programms verdeckt bleiben. Eine Zweckbestimmung, schon vorher in irgendeiner Weise erkannt zu werden bzw. in Erscheinung zu treten, haben sie nicht.

dd. Auch der Umstand, dass die zugunsten der Antragstellerin geschützte Marke "IBM" sowie die übrigen zum Gegenstand des Verfügungsantrags gemachten Kennzeichen in Datei-bezeichnungen der auf die Server der Antragsgegner hochgeladenen Datenpakete enthalten sind, reicht nach Auffassung des Senats nicht aus, eine Markenrechtsverletzung zu begründen. Die Antragsgegner haben vorgetragen, dass sie gerade die Dateinamen einer umfangreichen Überprüfung auf rechtsverletzende Markenbezeichnungen unterziehen und entsprechende Dateien sperren. Es ist insoweit für den Senat nicht ersichtlich, dass für diese konkrete Art der Beeinträchtigung ? die sich von der auf den Dateiinhalte bezogenen urheberrechtlichen Problematik maßgeblich unterscheidet ? weitergehende zumutbare Kontrollmöglichkeiten bestehen, um die Verwendung rechtsverletzender Datei-bezeichnungen zulasten der Antragstellerin vollständig auszuschließen. Auch der Umstand, dass im Anschluss an von der Antragstellerin erhobene Beanstandungen erneut z. B. die Markenbezeichnung "IBM" in Dateinamen aufgetaucht ist, belegt nicht eine Untätigkeit oder eine mangelnde Kontrolle durch die Antragsgegner. Die gegenüber der Rechtmäßigkeit des Geschäftsmodells der Antragsgegner bestehenden Bedenken des Senats beziehen sich nicht in gleicher Weise auf die Dateinamenbezeichnung. Denn diese liegen ? für eine Überprüfung und Filterung ? offen zu Tage. Ein Markenrechtsverstoß ist aus Sicht des Senats demgemäß nicht hinreichend wahrscheinlich.

c. Die Antragsgegner sind auch nicht als Teilnehmer einer Markenrechtsverletzung verantwortlich, die die unberechtigten Nutzer der Raubkopien in dem Moment begehen, in dem sie das Produkt erwerben und installieren. Denn insoweit fehlt ihnen ein hinreichend konkreter (doppelter) Gehilfenvorsatz. Insoweit wird zur Vermeidung unnötiger Wiederholungen auf die Ausführungen auf der Grundlage der Rechtsprechung des Bundesgerichtshofs zur Störerhaftung Bezug genommen.

17. Die Kostenentscheidung beruht auf §§ 97, 92 Abs. 2 ZPO.

Die Ergänzung des Antrags im Hinblick auf ein Handeln im Rahmen eines Online-Dienstes fällt kostenmäßig nicht ins Gewicht. Für die ausdrückliche ? und angesichts des Vorgehens der Antragstellerin in den Ordnungsmittelverfahren nicht nur klarstellende ? Beschränkung auf den Dienst www...com sowie die Abweisung hinsichtlich der markenrechtlichen Ansprüche hält der Senat eine Verlustquote zulasten der Antragstellerin von 20% für angemessen. Dabei ist berücksichtigt worden, dass der Streit der Parteien in rechtlicher Hinsicht ganz überwiegend urheberrechtliche Fragen betrifft und markenrechtliche Ansprüche ersichtlich nur am Rande geltend gemacht worden sind.