Zoning und Geolocation - Technische Ansätze zu einer Reterritorialisierung des Internet

Thomas **Hoeren** *

In der rechtlichen Diskussion vermehren sich die Stimmen, die auf technische Möglichkeiten zu einer Reterritorialisierung des Internet hinweisen. Es soll zunehmend möglich sein, den Zugriff des Internet auf bestimmte Regionen zu beschränken. Dadurch wären viele kollisionsrechtliche Probleme des Internetrechts gelöst. Der Beitrag untersucht die Möglichkeiten für eine solche Geolocation und zeigt die technischen Grenzen solcher Verfahren auf.

I. Einführung

Der Schock kam mit Yahoo!: Französische Studentengruppen fanden im Auktionsbereich des amerikanischen Providers Yahoo! Angebote zum Erwerb von Naziartikeln. Sie begehrten vor französischen Gerichten eine einstweilige Anordnung, in der Yahoo! aufgetragen wurde, alle erforderlichen Maßnahmen zu treffen, um französischen Internetnutzern den Zugriff auf Internetseiten mit NS-Devotionalien zu verwehren. Und sie bekamen Recht: Die französische Justiz [1] gewährte weltweit erstmals eine Art Reterritorialisierung des Internet, d.h. eine territoriale Beschränkungen des Zugriffs auf Internetseiten. Dabei stützte sich der französische Richter Gomez auf ein Gutachten, das zwei Franzosen sowie der amerikanische „Internet-Mitbegründer“ Vinton Cerf erstellt hatten. Demnach könne zu 70% gewährleistet werden, dass die fraglichen Seiten aus Frankreich nicht mehr aufgerufen werden, da die Nutzer auf Grund ihrer IP-Adresse eindeutig lokalisiert werden können.

Gomez verfügte daher, dass Yahoo! entsprechende IP-Sperren im Verhältnis zu französischen Nutzern vorsehen könne. Yahoo! wehrte sich heftig gegen diese Konzeption mit Verweis darauf, dass eine IP-Lokalisierung unmöglich, zumindest unverhältnismäßig aufwändig sei. US-amerikanische Gerichte lehnten daraufhin die Vollstreckung der französischen Entscheidung ab. [2] Doch die Frage der IP-Identifikation und ihrer Wirksamkeit blieb ungeklärt. Dies ist vor allem deshalb bedenklich, da eine solche Identifikation auch viele kollisionsrechtliche Fragen im Internetrecht technisch obsolet machen würde. Wenn es möglich ist, den Zugriff auf Websites territorial zu beschränken, kann man damit auch die Zielrichtung und den Marktort einer Website bestimmen. Dann wäre diese technische Vorgabe insofern auch wieder kollisionsrechtlich zu beachten, als dann der Aufbau einer Website eben nicht mehr dem Recht aller Staaten unterworfen werden kann, sondern nur der Rechtsordnung des jeweils technisch vorgegebenen Zielgebiets.

Das war die Geburtsstunde der Diskussion um Zoning und Geolocation. „Zoning“ bezeichnet die auf geografischen Kriterien basierte Steuerung des Informationszugangs und -inhalts im Internet. Zweck von Zoning soll es sein, Webinhalte zum einen auf den Kunden passgenau zuzuschneiden und ihm z.B. regionale Werbung einblenden zu können. Zum anderen sollen rechtliche Probleme gelöst werden, die sich aus den unterschiedlichen Jurisdiktionen ergeben (s.u.). Durch ein Zoning hätte ein Anbieter von Webdiensten die Möglichkeit, Nutzer aus bestimmten Bereichen auszuschließen. Ein Spezialfall des Zoning ist Geolocation oder Geo-Targeting. Darunter versteht man Verfahren, mit denen man IP-Adressen einem geografischen Ort zuordnen kann. [3] Bereits jetzt gibt es viele Anbieter, die Geolocation-Verfahren entweder selber einsetzen oder darauf aufbauende Produkte und Dienstleistungen anbieten. Neben der wirtschaftlichen Nutzung von Geolocation-Verfahren haben diese auch rechtliche und politische Auswirkungen. [4]

II. Rechtliche Bedeutung von Geolocation

Mit dem Thema Geolocation haben sich bislang erst wenige Juristen auseinander gesetzt. Anlass war entweder ein Gerichtsurteil, wie im Yahoo!-Fall (s.o.), oder das Thema wurde nur am Rande gestreift. [5] Geolocation-Verfahren sind überall dort von Bedeutung, wo es um die Herkunft von Internetnutzern geht. Denn damit lässt sich auch ein Ausschluss von Nutzern bewerkstelligen. Wichtig wären solche Verfahren z.B. für das Urheberrecht. Im Bereich des Rundfunk/Broadcasting werden Geolocation-Verfahren zunehmend wichtiger, da sich durch diese (relativ) genaue Ziel- bzw. Absatzgebiete festlegen lassen. Es ist also möglich, Onlineübertragungsrechte, z.B. von großen Sportveranstaltungen, länderspezifisch zu vermarkten.

Aber auch im B2C-Bereich hat diese Form der Rechteverwertung Auswirkungen. Dies zeigt sich z.B. beim Onlinevertrieb von Filmen, da diese auf Grund der immer größeren Verbreitung von Breitbanddiensten verstärkt über Server „verkauft“ werden. So lässt sich sicherstellen, dass sich Nutzer aus Deutschland einen

Kinofilm, der in den USA schon lange, aber in Deutschland noch nicht in den Kinos gelaufen ist, vorher anschauen können. Gleiches gilt für den Vertrieb von Musikstücken, die entweder überhaupt

nicht oder nicht zu diesem Zeitpunkt in einem bestimmten Land verfügbar sein sollen. Auch P2P-Netzwerke lassen sich so auf Staaten beschränken, in denen sie erlaubt bzw. nicht verboten sind.

Auch im Markenrecht, insbesondere im Domainrecht, kann Geolocation-Verfahren eine sehr große Bedeutung zukommen.[6] So lässt sich nämlich relativ leicht und wirksam eine komplette nationale Markenrechtsordnung ausschließen, da es am „commercial effect“ mangelt. Aber auch im Verwaltungs-/Ordnungswidrigkeits-/Strafrecht sind Geolocation-Verfahren bedeutsam. So kann u.U. verhindert werden, dass deutschen Nutzern rechtswidrige (NS-)Seiten angezeigt werden.[7] Aber auch Internetwettanbieter können so einen Zugriff auf ihre Angebote von Nutzern aus Staaten, in denen Onlinewetten verboten sind, verhindern und so staatlichen Maßnahmen entgehen.

Auch im Kartellrecht wäre Geolocation äußerst hilfreich.[8] Überall dort, wo es um die geografische Abgrenzung geht, liegt natürliche auch eine geografische Aufteilung von Märkten nahe, die dann kartellrechtlich relevant ist, wenn marktbeherrschende Unternehmen diese untereinander aufteilen.

Schließlich wirken sich Geolocation-Verfahren auf die internationale Zuständigkeit von Gerichten aus.[9] So lassen sich z.B. alle Zugriffe von außerhalb eines Landes abblocken, sodass nur einheimische Gerichte zuständig sein können, da in den anderen Staaten keine Verletzungshandlungen vorliegen können.

III. Derzeitige Anwendungsbeispiele

Zoning-Verfahren finden sich schon heute in der Internetwelt. Wenn man in Deutschland die Domain google.com aufrufen möchte, wird man automatisch auf die deutsche Website google.de umgeleitet. Bei der Eingabe von amazon.com oder ebay.com öffnet sich zwar die amerikanische Website, allerdings wird sofort gefragt, ob man nicht zu dem deutschsprachigen Ableger wechseln möchte.

PayPal nutzt Geolocation-Verfahren, um Onlinezahlungen auf regionale Unstimmigkeiten zu überwachen und so Betrug zu verhindern.[10] etracker verwendet Geolocation-Verfahren in seinen Produkten, um damit eine geografische Besucheranalyse bis hin zum „Web-Controlling“ zu ermöglichen.[11] Dabei greift etracker auf Produkte von Digital Envoy zurück und wirbt mit einer Genauigkeit von 99,8% auf Länder-, 92% auf Regional- und 88% auf Städteebene.[12] Der E-Mail-Service-Anbieter DidTheyReadIt zeigt, wann, wie lange und wo eine E-Mail gelesen wurde.[13]

Großer Beliebtheit erfreuen sich Geolocation-Verfahren in den Werbe- und Marketingbranchen.[14] So bieten DoubleClick und Google ihren Kunden die Schaltung regional differenzierter Werbung an.[15] Aber auch im Bereich des Digital Rights Managements (DRM) sind Geolocation-Verfahren im Einsatz, da die Rechteverwertung von Sportverbänden oder Filmverlagen territorial erfolgt.[16] Hingewiesen sei auch auf politisch motivierte Einsätze von Geolocation, etwa wenn die chinesische Regierung Geolocation nutzt, um die Bevölkerung von unerwünschten ausländischen Websites fernzuhalten.

IV. Technische Vorgaben

Die Internet Assigned Numbers Authoritiy (IANA)[17] versorgt alle fünf Regional Internet Registries (RIR) mit IP-Adressen.[18] Diese verwalten, verteilen und registrieren die im öffentlichen Internet bekannten und gerouteten IP-Adressen in ihren jeweiligen Regionen.[19] Für Europa ist das Réseaux IP Européens (RIPE),[20] ein Zusammenschluss europäischer Internetprovider, zuständig.[21] Die RIR weisen ihrerseits den Internet Service Providern (ISP) - den Besitzern - einzelne IP-Adressblöcke zu, die diese dann an ihre Nutzer vergeben.

Die Adressräume werden dabei durch die ersten 8 Bits einer Adresse (most significant byte) unterschieden. Eine Liste der aktuellen Zuordnung von Adressräumen an die regionalen Institutionen findet sich im Netz unter: http://www.iana.org/assignments/ipv4-address-space. Die fünf regionalen Institutionen vergeben nun wiederum innerhalb ihres Adressraums weitere Adressräume an nationale Institutionen, die National Internet Registries (NIR). Diese vergeben nun Adressbereiche an ISP wie z.B. T-Online und diese geben ihren Kunden, den Endnutzern, eine spezielle IP-Adresse. Diese IP-Adresse wird in der Regel dynamisch vergeben, d.h. dass ein Nutzer für eine Internetsession eine feste Adresse bekommt, die sich von Session zu Session ändert/ändern kann.

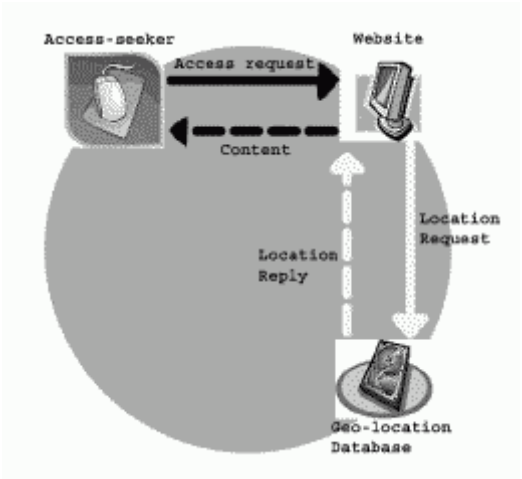
Die IANA und auch die RIR stellen Listen bereit, in denen die ISP mitsamt der Landeszugehörigkeit und dem ihnen verfügbaren IP-Adressbereich aufgelistet sind. Auf Grund dieser Listen lassen sich ohne größeren Aufwand Programme entwickeln, die einer IP-Adresse das entsprechende Land zuordnen. Diese Methode

funktioniert in den meisten Fällen exakt. Es gibt jedoch Ausnahmen, bei denen für eine IP-Adresse nicht das zugehörige Land ermittelt werden kann.

Nun lässt sich zwar nicht die exakte geografische Position der einzelnen Nutzer herausfinden. Allerdings sind die Besitzer der IP-Adressblöcke (ISP, Universitäten, etc.) aus öffentlich zugänglichen Quellen wie den Whois-Abfrageformularen der RIR bekannt.[22] Diese weisen die IP-Adressen einzelnen Netz-/Einwahlknoten zu. Diese Zuteilung wird meist nicht geändert, sodass die regionalen Einwahlknoten daher häufig einen eigenen festen IP-Adressen-Pool besitzen. Aus diesen Daten lässt sich dann eine Datenbank erstellen, die entweder die geografische Position einzelner IP-Adressen oder einzelner IP-Bereiche beinhaltet. Wenn nun der Websitebetreiber etwas über die Herkunft seiner Besucher wissen möchte, braucht er nur in der Datenbank

nachzuschauen, welchem Ort die übermittelte IP-Adresse des Besuchers zugeordnet ist.

Um an eine Lokalisierung des Nutzers zu gelangen, wird die IP mit Datenbanken bekannter IP-Adressen verglichen. Große Provider verteilen meistens ähnliche IP-Adressen oder Adressenbereiche an ihre Nutzer. Ferner können die vom Computer benutzten Router (also der Weg durchs Internet: „Routing Information“) zurückverfolgt und somit das Ursprungsland ausfindig gemacht werden. Inzwischen gelingt es nach Angaben der verschiedenen Anbieterdienste durch die Kombination dieser Methoden in 90-98 % der Fälle, das Ursprungsland ausfindig zu machen.[23] Eine Verdeutlichung der Funktionsweise bietet das Schaubild:[24]



Wie im Schaubild gezeigt, bekommt jeder, der sich in das Internet einwählt, eine weltweit eindeutige IP-Adresse für die Dauer seiner Internetnutzung. Diese erhält er von seinem ISP. Sie ist meist dynamisch, d.h. der ISP weist seinem Nutzer nicht immer die gleiche IP-Adresse zu, sondern irgendeine aus seinem IP-Adressen-Pool. Statische IP-Adressen werden hingegen fest einem bestimmten Nutzer zugewiesen.

Auf solchen Techniken setzen verschiedene Produkte auf. Das Programm Geoselect[25] der Fa. Geobytes macht sich z.B. Angaben der ISP über die Verteilung ihrer IP-Adressbereiche auf Länder und Städte zunutze und kann so das Herkunftsland und sogar die Stadt eines Internetnutzers herausfinden. Die Qualität der Ergebnisse von Geoselect hängt allerdings stark mit der Qualität der Informationen zusammen, die die ISP zur Verfügung stellen. Die Implementierung des Programms ist dagegen denkbar einfach. Es reichen einige HTML-Befehle aus, um gewünschte geospezifische Informationen zu erhalten.

DNSMIRROR[26] sammelt seit mehreren Jahren IP-Adressen und erfragt die Länder bei den zuständigen RIR, die diese verwalten. Weiterhin wertet DNSMIRROR sog. „Routing Informationen“ aus, mit deren Hilfe die Entfernungen der Surfer ermittelt und mit den gespeicherten Daten abgeglichen werden kann. Das Programm erreicht nach Angaben der Entwickler eine Genauigkeit von ca. 95%, um das Herkunftsland einer IP-Adresse zu bestimmen.

V. Ist Geolocation derzeit wirklich möglich?

In der rechtlichen Diskussion wird vermehrt behauptet, Geolocation scheitere an den technischen Möglichkeiten. Diese Behauptung ist unzutreffend und zutreffend zugleich, wie im Weiteren zu zeigen sein wird.[27] Am heftigsten kritisiert wird die Genauigkeit der genannten Technologien. Die ITAA (Information Technology Association of America) hat ein Essay über die Einsatzmöglichkeiten von Geolocation verfasst, in welchem sie feststellt, dass Geolocation-Systeme beim derzeitigen Stand der Technik für die Bestimmung des Herkunftslands einer Anfrage noch nicht hinreichend ausgereift sind.[28] Im Wesentlichen ergeben sich bei dem

Geolocation-System folgende zwei Problemgruppen: „source problems“ and „circumvention problems“.

1. „Source Problems“

Diese Probleme entstehen dadurch, dass die IP-Datenbanken ständig gepflegt und aktualisiert werden müssen.[29] Es gibt im Bezug auf IP-Adressen kein Äquivalent zum Telefonbuch oder sonstigen Registern für Adressen (Einwohnermeldeamtregister etc.).[30] Daher sind die Anbieter auf weniger verlässliche Daten wie Registrations-Datenbanken,[31] Network-Routing-Informationen, DNS-Systeme, Host-Name-Translations, ISP-Informationen und Webinhalte angewiesen.[32] Gerade in Bezug auf technisch weniger hoch entwickelte Regionen lässt sich eine regionale Eingrenzung anhand der IP-Adresse nur schwer durchführen, da im Gegensatz zu hoch technologisierten Gebieten selten IP-Adressblöcke für lokale Regionen reserviert werden.[33]

Problematisch wird es u.a. bei AOL-Nutzern zumindest in den USA, da AOL in Amerika einen zentralen Proxyserver benutzt, welcher auf einen Aufenthaltsort aller AOL-Nutzer in Virginia, dem Standort des Proxyservers hindeutet.[34] Im Wege einer Konzernneuausrichtung will sich AOL aber in Europa von seinem Zugangsgeschäft trennen.[35] Dies wurde in Deutschland von der Telecom Italia[36] und in Frankreich vom Festnetzanbieter Neuf Cegetel[37] übernommen. Auch in Großbritannien gibt es bereits Interessenten.[38] Damit wird sicherlich auch eine Infrastrukturumstellung einhergehen, sodass zumindest von den ca. 6 Mio. ehemaligen europäischen AOL-Kunden leichter die Herkunft bestimmt werden kann.

Ein weiteres Problem wird die Umstellung des IP-Adressverfahrens von IPv4 auf IPv6 mit sich bringen. IPv4 bietet ca. 4,25 Mrd.[39] verschiedene IP-Adressen, mit IPv6 lassen sich theoretisch $3{,}4\times10^{38}$ Adressen[40] bilden. Da die 4,25

Mrd. verfügbaren Adressen im IPv4-System u.U. in absehbarer Zukunft nicht mehr ausreichen werden, um den Internetverkehr aufrechtzuerhalten,[41] hat eine Umstellung auf IPv6 bereits begonnen.[42] Im IPv4-System ist es äußerst umständlich, vergebene IP-Adressen umzuverteilen, da eine solche Maßnahme stets ein Nachkonfigurieren von Routern und Servern nach sich zieht.[43] Im IPv6-System sind Umadressierungen schnell und einfach möglich, was unweigerlich dazu führen wird, dass die IP-Datenbanken der Geolocation-Anbieter schwerlich stets auf dem aktuellsten Stand sein werden. Gerade in der Umstellungszeit von IPv4 auf IPv6, wenn beide Systeme noch simultan benutzt werden, ist eine Erstellung verlässlicher Datenbanken nahezu undenkbar. Da den Unternehmen wie oben gezeigt jedoch lediglich anhand ihrer Datenbanken ein Rückschluss auf den Aufenthaltsort des Internetnutzers ermöglicht wird, bestehen große Zweifel an der Einsatzmöglichkeit des Verfahrens für rechtlich bedeutsame Entscheidungen.

2. „Circumvention Problems“ (Umgehungsprobleme)

Ferner ergeben sich Probleme daraus, dass die Lokalisation anhand der IP-Adresse mit relativ wenig Aufwand umgangen werden kann. Zum einen besteht die Möglichkeit, mithilfe von Tools die IP-Adresse zu verschleiern[44] bzw. über eine telefonische Einwahl bei einem im Ausland befindlichen Provider ins Internet zu verbinden.[45] Die telefonische Einwahl bei ausländischen Providern führt zu derart hohen Telefonkosten, dass sie keine wirkliche Alternative darstellt. Die Benutzung der Tools hingegen ist relativ einfach. Im Wesentlichen ermöglichen die Tools einen Zugriff auf Proxyserver, über welche dann jede Anfrage ins Internet geschickt wird. Auf Grund dessen erkennt das Geolocation-System lediglich den Standort des Proxyservers, niemals jedoch den Standort des „Endnutzers“.[46] Zum anderen bestehen neben diesen relativ einfachen Umgehungsmethoden weitere, die vertieftes Internet-Know-how erfordern, im Falle der Implementation dann aber auch sehr effektiv gegen eine Lokalisation durch Geolocation-Systeme schützen.[47]

Manche ISP wie T-Online bieten neben dem herkömmlichen Zugang auch einen Zugang für Kunden im Ausland an. Ein T-Online-Kunde kann so z.B. von einem Rechner in Frankreich aus mit einer IP-Adresse surfen, die ihm von T-Online zugeteilt wird. Versucht man nun die Herkunft dieser IP-Adresse zu ermitteln, so erhält man als Ergebnis das Land Deutschland. Eine weitere Möglichkeit zur Verschleierung seiner IP-Adresse sind sog. Rewebber-Dienste. Hierfür ruft man einfach die Seite des Rewebbers auf, gibt in der entsprechenden Zeile die URL der Seite ein, die man eigentlich besuchen will und schon wird dieser Seite eine „falsche“ IP-Adresse übermittelt, nämlich die des Rewebbing-Servers. Ein solcher Rewebber ist z.B. unter: http://anonymouse.org zu finden.

3. Zusammenfassung der Kritik

Somit bestehen (derzeit noch) ernstliche Zweifel an der Verlässlichkeit der Datenbanken, den angewandten Methoden und den daraus resultierenden Ergebnissen. Aus juristischem Blickwinkel betrachtet scheint es so,

dass Geolocation keine tauglichen Ergebnisse liefern kann, an welche weitreichende Folgen geknüpft werden können. 48

VI. Schlussüberlegung: Sinnvolle Einsatzgebiete

Da ein Einsatz für rechtlich relevante Weichenstellungen derzeit nicht in Betracht kommt, ist fraglich, inwieweit die beschriebenen Verfahren anderweitig genutzt werden können. Festzustellen ist, dass Geolocation bereits in vielen Bereichen benutzt wird: Wichtige Beispiele sind regional angepasste Werbung, 49 Überwachung von Onlinezahlungen auf regionale Unstimmigkeiten zwecks Betrugsschutzes, Marktanalyse, Spam- und Phishing-Schutz, Bestimmen der vom Nutzer benutzten Währung oder Sprache beim Besuch der Websites. 50 Da in diesen Bereichen ein Fehler, der z.B. auf unkorrekten Daten beruht, keine verheerende Wirkung hätte, ist die derzeitige Genauigkeitsrate für die Anwendung dort ausreichend. 51

Ferner würde die Möglichkeit, spezielle Regionen ausgrenzen zu können, die Vermeidung von Lizenzverstößen ermöglichen, wenn diese z.B. regional vergeben wurden. Außerdem kommen Beschränkungen auf Grund regionaler Zugehörigkeit für Nutzer von Gambling-Seiten und Pharmavertriebsseiten in Betracht, um ein globales Tätigwerden unter Einhaltung lokaler Regelungen zu ermöglichen. Da jedoch, wie oben dargelegt, erhebliche Bedenken an der Verlässlichkeit der Technologie bestehen und Verstöße in diesen Bereichen durchaus schwerwiegende Konsequenzen für einen Anbieter zur Folge haben können, ist ein Einsatz von Geolocation in den letztgenannten Bereichen (noch) nicht angezeigt.

Im Ergebnis ist es durchaus mit geringem Aufwand möglich, die Herkunft einer IP-Adresse zu bestimmen. Es gibt jedoch noch keine Möglichkeit, dies mit hundertprozentiger Sicherheit zu tun. Die meisten Programme zur Bestimmung der Herkunft einer IP-Adresse verwenden Listen, die von den RIR oder ISP bereitgestellt werden. Daher hängt die Qualität eines Local Identifiers mit der Qualität und Vollständigkeit dieser Listen eng zusammen. Die Auswertung von Routinginformationen, wie es das Programm von DNSMIRROR macht, kann zu einer Verbesserung der Ergebnisse führen. Local Identifier lassen sich durch die Benutzung von Proxyservern oder Rewebbern täuschen.

Es ist also für jemanden mit dem nötigen technischen Know-how jederzeit möglich, seine Herkunft im Internet zu verschleiern. Sollte z.B. eine Webseite - wie im einleitend geschilderten Yahoo!-Fall - für alle französischen Nutzer gesperrt werden, so lässt sich dies für den Großteil aller französischen Nutzer auch bewerkstelligen. Es wäre jedoch nicht möglich, wirklich alle französischen Nutzer auszuschließen.

---

* Professor Dr. Thomas **Hoeren** ist Direktor der zivilrechtlichen Abteilung des Instituts für Informations-, Telekommunikations- und Medienrecht (ITM) an der Universität Münster.

1 Vgl. dazu TGI, K&R 2000, 365 ff.; TGI K&R 2001, 63 f. m. Anm. Hartmann; TGI MMR 2001, 309 (Ls.) m. Anm. Namgalies; U.S. District Court for the Northern District of California MMR 2002, 26 ff. m. Anm. Mankowski; Hilger, MMR 3/2006, S. XIV.

2 U.S. District Court for the Northern District of California MMR 2002, 26 - Yahoo v. LICRA. Inzwischen hat es in den USA ein weiteres Tauziehen um dieses Urteil gegeben, das im Mai 2006 mit einer Entscheidung des Supreme Court endete, die eine Intervention zu Gunsten von LICRA ablehnte und damit faktisch Yahoo! von der Rechtsverfolgung verschonte.

3 K. Köhntopp/M. Köhntopp/Seeger, K&R 1998, 25, 29 hielten dies noch für unmöglich.

4 Dazu unten II.

5 Ott, Urheber- und wettbewerbsrechtliche Probleme von Linking und Framing, 2004, S. 164 ff.

6 S. dazu BGH MMR 2005, 239 - HOTEL MARITIME.

7 S. dazu Engel, MMR-Beilage 4/2003; Mankowski, MMR 2002, 277 und Stadler, MMR 2002, 343 ff. Zum Stand der derzeitigen Massenverfahren s. OVG Münster MMR 2003, 348 mit Anm. Spindler/Volkmann; VG Köln MMR 2003, 205 mit Anm. Stadler und VG Köln MMR 2005, 399 m. Anm. Kazemi.

8 S.a. dazu das BMBF-Forschungsprojekt Internetökonomie, das sich am Institut für Informations-, Telekommunikations- und Medienrecht (ITM) mit Fragen der räumlichen Marktabgrenzung im Internet beschäftigt; http:// www.uni-muenster.de/Jura.itm/**hoeren**/ Rubrik „Projekte“.

9 KG CR 1997, 685; dazu auch u.v.a. Koch, CR 1999, 121; High Court of Justice CRI 2005, 21.

10 Krüger, Kanäle im Netz, http://www.heise.de/tp/r4/artikel/18/18005/1.html; http://de.wikipedia.org/wiki/Geolocation; http://meineipadresse.de/html/geolocation.php.

11 http://de.wikipedia.org/wiki/Geolocation.

12 http://www.etracker.de/layoutAPI?id=MainPageB1500; http://www. etracker.de/layoutAPI?id=MainPageS1800.

13 http://didtheyreadit.com/index.php; Krüger (o. Fußn 10); http://de. wikipedia.org/wiki/Geolocation.

14 Krüger (o. Fußn. 10).

15 https://adwords.google.de/select/targeting.html; http://de.wikipedia.org/wiki/Geolocation.

16 Krüger (o. Fußn. 10).

17 http://www.iana.org.

18 http://www.heise.de/newsticker/meldung/77925.

19 http://www.heise.de/glossar/entry/3eed80c1a59b0f62.

20 http://www.ripe.net.

21 http://www.heise.de/glossar/entry/f234dac2d497404f.

22 Lischka, Zensur und Werbung, http://www.heise.de/tp/r4/artikel/4/4349/1.html.

23 Goldsmith/Sykes, The Internet and the dormant Commerce Clause, 110 Yale L.J. 785, 811; Anbieter behaupten noch höhere Erfolgsquoten: 99,9% bzgl. des Landes, 90% bzgl. des US-Staates, vgl. http://www.quova.com/file.php?id=25; Digital-Element spricht sogar von 99% bzgl. des Landes und 94% bzgl. der genauen Stadt, weltweit, vgl. http://www.digital-element.net/ip_intelligence/ip_intelligence.html.

24 http://svantesson.org/svantesson4geohow.htm.

25 http://www.geobytes.com/GeoSelect.htm.

26 http://www.dnsmirror.de/.

27 Goldsmith/Sykes (o. Fußn 23), 785, 809 ff.

28 Information Technology Association of America (ITAA), ECommerce Taxation and the Limitations of Geolocation Tools, http://www.itaa.org/taxfinance/docs/geolocationpaper.pdf. Ansatzpunkt war die Einsatzmöglichkeit des Geolocation zur Bestimmung des Heimatlands eines Käufers bei E-Transactions, wonach eine Entscheidung über eine Besteuerung der Transaktion gefällt werden kann; i.E. ebenso: Finkelstein, Expert Report of Seth Finkelstein, http://www.sethf.com/nitke/ashcroft.php.

29 Svantesson, Geo-identification - Now They Know Where You Live, Privacy Law & Policy Reporter, Vol. 11 No 6, p. 3, http://epublications.bond. edu.au/law_pubs/12/.

30 Svantesson (o. Fußn. 29).

31 http://www.aso.icann.org/rirs/.

32 Svantesson (o. Fußn. 29); Ausf. Diskussion in: Edelman, Shortcomings and Challenges in the Restriction of Internet Retransmissions of Over-the-air Television Content to Canadian Internet Users, http://cyber.law.harvard.edu/people/edelman/pubs/jump-091701.pdf.

33 ITAA (o. Fußn. 28), S. 4.

34 Meta Group, Perils, promises of geolocation (Stand: 19.4.2001), http://news.com.com/2009-1023_3-256139.html; Yahoo!, Inc. v. LICRA, 433 F.3d 1199, 1247 (9th Cir. 2006).

35 http://www.heise.de/newsticker/meldung/71993.

36 http://www.heise.de/newsticker/meldung/78302.

37 http://www.heise.de/newsticker/meldung/78497.

38 http://www.heise.de/newsticker/meldung/78814; http://www.heise.de/newsticker/meldung/78497.

39 Olsen, Geographic tracking raises opportunities, fears (Stand: 8.11.2000), http://news.com.com/2100-1023_3-248274.htm.

40 http://www.rvs.uni-bielefeld.de/~heiko/tcpip/tcpip_html_alt/kap_3_1.html.

41 http://www.heise.de/newsticker/meldung/78095 (Stand: 8.9.2006); http:// www.heise.de/newsticker/meldung/77925.

42 ITAA (o. Fußn. 28), S. 6 f.

43 ITAA (o. Fußn. 28), S. 7.

44 Z.B. http://www.anonymizer.com; http://www.silentsurf.com.

45 Goldsmith/Sykes (o. Fußn. 23), 785, 811.

46 Edelman (o. Fußn. 32), S. 8, http://cyber.law.harvard.edu/people/edelman/pubs/jump-091701.pdf.

47 Z.B. sog. „deep linking to streaming video content without accessing the HTTP server“ oder „tunnelling methods“, Svantesson (o. Fußn. 29); Edelman (o. Fußn. 32), S. 9 f. Zu beachten ist jedoch, dass solches Fachwissen sehr schnell und effektiv z.B. in Internetforen an weniger erfahrene Nutzer weitergegeben und durch die Erstellung von kurzen Anleitungen auch von diesen leicht benutzt werden kann. Beim „deep linking“ bedarf es nämlich i.d.R. lediglich des direkten Links zu den „streaming-contents“, welcher folglich in den Foren gepostet werden und genutzt werden kann.

48 Wie z.B. straf- oder urheberrechtliche Konsequenzen oder die Bestimmung der zuständigen Jurisdiktion.

49 Z.B. https://adwords.google.de/select/targeting.html.

50 Vgl. http://www.geo-targeting.de.

51 Auch wenn die angegebenen Raten (o. Fußn. 3) schwer nachweisbar sind. ITAA (o. Fußn. 28), S. 5 f. stellt fest: „There is no way to independently verify whether the software could provide the claimed levels of accuracy if the software vendors didn’t first have other customer location information which their software may be using to determine customer location.“; zu den Begriffen: „false negatives“ und „false positives“: Edelman (o. Fußn. 32), S. 6 f.