



**Stellungnahme zur Anhörung
des Ausschusses für Wirtschaft und Technologie
im Deutschen Bundestag**

am 11. Dezember 2006

**zum Elektronischer-Geschäftsverkehrs-Vereinheitlichungs-Gesetz (EIGVG),
insb. Entwurf eines Telemediengesetzes (TMG) – (Drs. 16/3078)**

**sowie zum diesbezüglichen Antrag der Fraktion Bündnis 90/Die Grünen
(Drs. 16/3499)**

eBay bedankt sich für die Einladung zur Stellungnahme im Gesetzgebungsverfahren für ein Elektronischer-Geschäftsverkehrs-Vereinheitlichungs-Gesetz (EIGVG), das insbesondere das neue Telemediengesetz des Bundes einschließt.

Die mit dem Gesetzentwurf umgesetzte Neuordnung der Kompetenzen zwischen Bund und Ländern im Bereich der Tele- und Mediendienste ist nachdrücklich zu begrüßen. Der Entwurf schreibt weithin den durchaus bewährten Rechtsrahmen für den elektronischen Geschäftsverkehr fort.

Leider wurden aber einige wesentliche Regelungsfragen, die sich in der Erfahrung der letzten Jahre als problematisch erwiesen haben, nicht angerührt. Dies sollte, wenn wegen des Zeitdrucks nicht im jetzigen Verfahren, so doch zumindest in einer sich kurzfristig anschließenden Fortentwicklung des neuen TMG geschehen. Für die Anhörung seien aus den Fragen drei Punkte exemplarisch herausgegriffen:

- *Mit Blick auf die Verantwortlichkeit von Host Providern für rechtsverletzende Inhalte Dritter hat sich eine Rechtsprechung entwickelt, die durch die Auferlegung weitreichender Überwachungspflichten nicht mehr im Einklang mit den Vorgaben der grundlegenden E-Commerce-Richtlinie der Europäischen Union steht.*
- *Ebenso fehlt die Umsetzung der Vorgaben der europäischen Kommunikations-Datenschutz-Richtlinie zur Datennutzung für die elektronische Werbeansprache im Rahmen bestehender Kundenbeziehungen (opt-out-Privileg).*
- *Schließlich ist den verschiedenen Forderungen nach einer Verschärfung des Koppelungsverbots in § 12 Abs. 3 TMG-E eine klare Absage zu erteilen, da sonst nicht nur erheblicher wirtschaftlicher Schaden droht, sondern auch massive Gefahren für den Verbraucherschutz zu befürchten sind.*

Die mit dem EIGVG verfolgte Neuordnung des Teledienste- und Mediendiensterechts in Deutschland ist grundsätzlich zu begrüßen. Insbesondere das Bemühen – im Zusammenwirken mit dem 9. Rundfunk-Änderungsstaatsvertrag der Länder – um eine nicht mehr nach kaum unterscheidbaren Dienstetypen, sondern nach Regelungsinhalten trennende Kompetenzverteilung zwischen Bund und Ländern ist ein wichtiger und richtiger Fortschritt, der durch diese Gesetzgebung erreicht wird.

Im Übrigen beschränkt sich das neugefasste Gesetz in weiten Teilen darauf, die bisherigen Regelungen aus Teledienstegesetz und Teledienste-Datenschutzgesetz fortzuschreiben. Dies ist nicht grundsätzlich zu kritisieren, hat sich doch gerade das TDG als ein wichtiges und wirksames Fundament für die Entwicklung des Internets und der Dienste der Informationsgesellschaft erwiesen. Es war daher richtig – und vor dem Hintergrund der den Rahmen bildenden eCommerce-Richtlinie auf europäischer Ebene auch bei vielen Fragen notwendig –, bestehende Grundregelungen beizubehalten.

Allerdings hat der lange Entstehungsprozess des Gesetzentwurfs – nicht zuletzt wegen der komplexen Beratungssituation mit Bund und Ländern – die Bereitschaft vermissen lassen, sich einigen Anpassungsnotwendigkeiten im Detail zu widmen. Hier wurde die Gelegenheit versäumt, aus den Erfahrungen nach einigen Jahren, in denen der elektronische Geschäftsverkehr in Deutschland an Verbreitung und Reife gewonnen hat, notwendige Schlüsse zu ziehen und Korrekturen oder Optimierungen durchzuführen.

Sofern jedoch wegen des erheblichen Zeitdrucks durch das parallele Staatsvertragsverfahren der Länder erforderliche Änderungen nicht mehr in diesem Gesetzgebungsverfahren durchgeführt werden können, erscheint es für einen Übergangszeitraum vertretbar, zunächst den vorliegenden Gesetzentwurf umzusetzen; im Anschluss sollte dann aber umgehend mit den ausstehenden inhaltlichen Überarbeitungen begonnen werden.

Im Einzelnen betrifft dies – neben zahlreichen anderen Punkten – insbesondere die folgenden drei für die Anhörung herausgegriffenen Fragen:

➤ **§ 7 ff. TMG-E: Verantwortlichkeit**

Die Regeln zur Verantwortlichkeit von Diensteanbietern sind von zentraler Bedeutung für die Entwicklung des elektronischen Geschäftsverkehrs und der Informationsgesellschaft, da erst dies das arbeitsteilige Zusammenwirken der verschiedenen technischen Dienstleister und Inhaltenanbieter im Internet ermöglicht. Im Rahmen der dreistufigen Gliederung von Internetdiensteanbietern ist eBay hinsichtlich der von unseren Nutzern eingestellten Angebote und Inserate als Host Provider gemäß § 10 TMG-E einzustufen.

Das spezielle Verantwortlichkeitsregime steht auch in keinem Widerspruch zu dem von eBay nachdrücklich unterstützten Ziel, eine wirksame Durchsetzung des Rechts im Internet, auch gerade einen starken Schutz geistiger und gewerblicher Schutzrechte sicherzustellen.

Es ist daher zu begrüßen, dass auch das TMG gemäß § 7 Abs. 2 TMG-E an dem bisherigen Grundprinzip festhalten soll, dass Diensteanbieter von ihnen nur gespeicherte oder übermittelte Informationen weder zu überwachen noch nach Umständen zu forschen haben, die auf eine rechtswidrige Tätigkeit hinweisen.

Dieser zentrale Grundsatz, der notwendige Grundlage jeder Betätigung als Diensteanbieter zur Speicherung oder Übermittlung von Internet-Inhalten ist, steht zurzeit im deutschen Recht erheblich in Frage. Die Entwicklung der Rechtsprechung, namentlich das BGH-Urteil vom 11. März 2004 in der Sache Rolex ./ ricardo (I ZR 304/01), führen zu erheblichen Schwierigkeiten und Unsicherheiten für Internetdiensteanbieter, die fremde Inhalte speichern (Host Provider). Entgegen den von der E-Commerce-Richtlinie vorgegebenen Prinzipien wurden den Anbietern hierdurch weitreichende Überwachungs- und Prüfpflichten und daraus resultierende Rechtsunsicherheiten aufgebürdet, die geeignet sind, allgemein anerkannte und erwünschte Dienstleistungen in Frage zu stellen.

Die Vorgabe des BGH, nach der der Diensteanbieter nach Hinweis auf eine Rechtsverletzung nicht nur das konkrete, rechtsverletzende Angebot unverzüglich sperren, sondern auch Vorsorge dafür treffen muss, dass es nicht zu weiteren entsprechenden Rechtsverletzungen kommt, führt faktisch zu einer in der Praxis nicht erfüllbaren Überwachungspflicht für fremde Inhalte.. Diese Rechtsprechung widerspricht der Regelungsintention nicht nur des deutschen Gesetzgebers, sondern auch den Vorgaben der E-Commerce-Richtlinie und bewirkt deshalb eine erhebliche Belastung und Rechtsunsicherheit hinsichtlich der Haftung von Internetdiensteanbietern für fremde Inhalte.

So bleibt unklar, welche Reichweite diese Monitoringpflichten haben können, ob und in welchem Grade Rechtsverletzungen als solche erkennbar sein müssen und wie mit der oft unklaren Reichweite geistiger und gewerblicher Schutzrechte umzugehen ist. Nur beispielhaft seien hier Fälle erwähnt, in denen sich eBay im Nachgang der BGH-Entscheidung Forderungen ausgesetzt sah, Möbelnachbauten anhand eines „händischen“ Bildvergleichs von Verkaufsangeboten mit Fotoaufnahmen des Herstellers zu beurteilen oder sich eBay über mehrere Instanzen der Frage stellen musste, ob der Weiterverkauf von Parfümtestern eine Markenrechtsverletzung darstellt oder nicht, obwohl dies von der Mehrzahl der befassten Land- und Oberlandesgerichte abgelehnt wurde.

Schon in jedem einzelnen Fall einer solchen auf Störerhaftung basierten „Unterlassungsverpflichtung“ stellen sich erhebliche Probleme. Denn der Einsatz von Filtern allein ist nicht ausreichend, da deren auf Schlagworten basierende Technik keine hinreichend eindeutige Identifikation rechtsverletzender Inhalte gewährleisten kann. Die notwendige manuelle Kontrolle, um Zweifelsfälle zu beurteilen, vom Filter unbeanstandete, aber rechtsverletzende Inhalte zu finden, andererseits aber auch Filtermeldungen von tatsächlich unbedenklichen Inhalten (sog. „falsche Positive“) auszusortieren, bedeutet einen nicht leistbaren Aufwand, wenn man sich etwa vor Augen führt, dass auf dem eBay-Marktplatz weltweit ständig ca. 78 Millionen Angebote auf der Seite sind und täglich etwa 8 Millionen neue Angebote eingestellt werden. Die Unzulänglichkeit automatischer Suchfunktionen wurde auch schon von der Europäischen Kommission im ersten Evaluierungsbericht zur E-Commerce-Richtlinie ausdrücklich bestätigt und in direktem Zusammenhang mit dem Verbot von Monitoring-Pflichten gesehen: *„[Das Fehlen allgemeiner Überwachungspflichten] ist wichtig, da eine systematische Überwachung von Millionen von Sites und Webseiten praktisch unmöglich ist und für die Vermittler eine unverhältnismäßige Belastung darstellen und für die Nutzer höhere Kosten für den Zugang zu grundlegenden Diensten bedeuten würde. (...) In diesem Zusammenhang sei darauf hingewiesen, dass es den Berichten und Studien über die Wirksamkeit von Sperr- und Filteranwendungen zufolge noch keine Technik gibt, die nicht umgangen werden könnte und absolut wirksam unerlaubte und schädliche Informationen blockiert und filtert, aber gleichzeitig vermeidet, dass völlig legale Informationen gesperrt werden, was einen Verstoß gegen das Recht auf freie Meinungsäußerung bedeuten würde.“*

Völlig unhaltbar wird die Situation aber durch die zu erwartende Kumulation zahlreicher Unterlassungsbegehren, weil es nicht bei Unterlassungspflichten hinsichtlich einzelner Artikel (z.B. Rolex Uhren) bzw. Rechtsverletzungen bleiben wird. Durch immer neu hinzukommende Verpflichtungen (die zeitlich nicht beschränkt sind) kommt es am Ende zu eben jener allgemeinen Monitoring-Pflicht für den Host Provider, wie sie doch gerade durch Art. 15 E-Commerce-Richtlinie und ebenso den bisherigen § 8 Abs. 2 TDG und künftigen § 7 Abs. 2 TMG-E ausgeschlossen sein soll.

Abhilfe kann insoweit auch nicht die tatbestandliche Einschränkung des Unterlassungstenors auf technisch mögliche und zumutbare Maßnahmen schaffen. Diese völlig ungewohnte Tenorierung mit einem eigenen einschränkenden Tatbestandsmerkmal führt nicht nur zu einer rechtssystemwidrigen Verlagerung wesentlicher Teile des gerichtlichen Er-

kenntnisverfahrens in das Vollstreckungsverfahren, sondern überdies zu einer nicht absehbaren Mehrbelastung der Gerichte. Denn in jedem Einzelfall, in dem ein rechtsverletzender Inhalt erscheint, müsste von einem Vollstreckungsgericht geprüft werden, ob ein Fall der Zuwiderhandlung vorliegt und ein entsprechendes Ordnungsgeld zu verhängen ist. Dazu müsste jeweils unter Hinzuziehung technischer Sachverständiger die Leistungsfähigkeit eingesetzter Filterprogramme bewertet und beurteilt werden, ob der Diensteanbieter bei Anlegung eines branchenüblichen Sorgfaltsmaßstabes tatsächlich sämtliche Suchbegriffe in die Filtersoftware eingegeben hatte, von denen zu erwarten war, dass sie für die Bewerbung des jeweiligen Artikels verwendet werden. Die sich hieraus ergebenden Abgrenzungsschwierigkeiten und die mit einer solchen Prüfung für den Diensteanbieter verbundene Rechtsunsicherheit sollte mit der gemeinschaftsweiten Einführung einer Haftungsprivilegierung aber gerade beseitigt werden.

Art. 15 der E-Commerce-Richtlinie stellt ausdrücklich fest, dass es keine allgemeinen Überwachungspflichten geben darf. Diese politische Grundentscheidung droht nun durch eine Fehlinterpretation der gemeinschaftsrechtskonform eng auszulegenden Ausnahmeregelung in § 8 Abs. 2 Satz 2 TDG (künftig § 7 TMG) ausgehöhlt zu werden. Diese Norm ist in ihrer Allgemeinheit missverständlich formuliert. Sie setzt im Hinblick auf Host-Provider Artikel 14 Abs. 2 der Richtlinie um. Im Gegensatz zum TDG spricht diese Vorschrift allerdings eindeutig nur von Verpflichtungen zur Entfernung oder Sperrung einer bestimmten Information. Auch der 47. Erwägungsgrund der Richtlinie, der Art. 15 konkretisiert, spricht in der insoweit deutlich präziseren englischen Sprachfassung der Richtlinie nur von der Möglichkeit zur Überwachung „in a specific case“.

Deshalb sollte auch der künftige § 7 Abs. 2 Satz 2 TMG-E lediglich die Entfernung oder Sperrung solcher Informationen erfassen, die zum Zeitpunkt der Beanstandung durch den in seinen Rechten Verletzten bereits dem Zugriff des Diensteanbieters unterliegen.

Zur Klarstellung der von der E-Commerce-Richtlinie vorgegebenen Maßstäbe ist daher folgende Ergänzung des § 7 Abs. 2 TMG-E erforderlich::

„(2) Diensteanbieter im Sinne des §§ 8 bis 10 sind nicht verpflichtet, die von ihnen übermittelten oder gespeicherten Informationen zu überwachen oder nach Umständen zu forschen, die auf eine rechtswidrige Tätigkeit hinweisen. Verpflichtungen nach den allgemeinen Gesetzen zur Entfernung oder Sperrung der Nutzung rechtswidriger Informationen ~~nach den allgemeinen Gesetzen, die zum Zeitpunkt der Beanstandung durch den Rechtsinhaber dem Zugriff des Diensteanbieters unterliegen~~, bleiben auch im Falle der Nichtverantwortlichkeit des Diensteanbieters nach den §§ 8 bis 10 ~~9 bis 14~~ unberührt. (...)“.

Sofern aufgrund des knappen Zeitplans des laufenden Gesetzgebungsverfahrens die notwendigen Änderungen im Moment nicht möglich sein sollten, müsste eine Anpassung im genannten Sinne jedenfalls Gegenstand einer möglichst kurzfristig anzugehenden zukünftigen Überarbeitung des TMG sein.

Eine solche zukünftige Überarbeitung sollte dann auch in der Verantwortlichkeitsregel für Host Provider (§ 10 TMG-E) klarstellen, worauf sich die Kenntnis von rechtswidrigen Inhalten beziehen muss (Inhalt und seine Rechtswidrigkeit, wie sich auch klar aus der französischen Sprachfassung der eCommerce-Richtlinie ergibt). Zudem sind in dieser Vorschrift konkretere Anforderungen an Art und Form einer kenntnisbegründenden Mitteilung einer Rechtsverletzung zu formulieren, da sich auch hier in der Praxis immer wieder erhebliche Rechtsunsicherheiten wegen völlig unzureichender Meldungen zeigen.

Schließlich sollte über die Einführung eines Meldeverfahrens für Rechtsverletzungen (Notice-and-Takedown-Verfahrens) nachgedacht werden, da dieses in besonderer Weise geeignet ist, sowohl den Interessen betroffener Rechteinhaber auf eine schnelle

Abstellung von Rechtsverletzungen als auch den Notwendigkeiten durch die automatisierte Datenverarbeitung im elektronischen Geschäftsverkehr Rechnung zu tragen. Wesentlicher Vorteil für die Rechteinhaber ist bei einem solchen Verfahren, dass ihrer Meldung bei Einhaltung bestimmter formaler Kriterien ein Vertrauensvorschuss entgegengebracht wird, der eine sofortige Beendigung der behaupteten Rechtsverletzung ermöglicht. Gleichzeitig wird so der vermittelnde Diensteanbieter aus der Richterrolle entlassen, die ihm zurzeit aufgedrängt wird, für die er aber weder die fachlich noch die institutionelle Kompetenz besitzt. Um auf der anderen Seite keine unberechtigte dauerhafte Beschränkung der Handlungs- und Meinungsfreiheit im Internet zu riskieren, muss ein Widerspruchsverfahren („Counternotice“) dem Anbieter des inkriminierten Inhalts die Möglichkeit geben, der Sperrung seines Inhalts entgegenzutreten und den Streit mit dem Meldenden einer gerichtlichen Klärung zuzuführen.

➤ **Datenschutz: Bestandsdatennutzung zur Werbeansprache (§§ 11, 14 TMG-E)**

Die Regelung zu den Bestandsdaten lässt im Entwurf die – europarechtlich zwingende – Umsetzung des Art. 13 Abs. 2 der Richtlinie zum Datenschutz in der elektronischen Kommunikation vermissen, wie sie etwa auch im Rahmen der TKG-Novelle in § 95 Abs. 2 TKG-2004 erfolgt ist. Art. 13 Abs. 2 der besagten Richtlinie stellt klar, dass in Abweichung von dem in Abs. 1 grundsätzlich festgeschriebenen opt-in-Prinzip innerhalb bestehender Kundenbeziehungen eine Nutzung der Kundendaten zur Ansprache per elektronischer Post grundsätzlich erlaubt ist und nur eine Widerspruchsmöglichkeit gegeben sein muss (opt-out). Diese Regelung wurde in § 7 Abs. 3 des neuen UWG auch in das deutsche Wettbewerbsrecht umgesetzt; diese UWG-Änderung bleibt aber ohne Wirkung auf die Frage der datenschutzrechtlichen Zulässigkeit der Datennutzung. Während das in der Richtlinie geregelte Prinzip im allgemeinen Datenschutzrecht nach § 28 Abs. 4 BDSG bereits allgemeines Prinzip ist, gelten bisher gerade in dem eigentlichen Regelungsbe- reich der Richtlinie, der elektronischen Kommunikation, strengere Grundsätze. Dies wurde im Rahmen der TKG-Novelle durch Einfügung des § 95 Abs. 2 TKG (mit Übernahme des Wortlautes aus § 7 Abs. 3 UWG) bereits korrigiert. Es ist zur vollständigen Richtlinien- Umsetzung nun aber auch notwendig, eine entsprechende Regelung auch im Daten- schutzrecht für die Telemedien zu verankern. Anderenfalls entstünde eine nicht zu rechtfertigende und überdies europarechtswidrige Benachteiligung von Telemedien im Vergleich zu allen sonstigen Wirtschaftsbranchen.

Es ist daher in § 14 TMG-E folgender neuer Absatz 2 einzufügen:

„(2) Ein Diensteanbieter, der im Rahmen einer bestehenden Kundenbeziehung rechtmäßig Kenntnis von der Rufnummer oder der Postadresse, auch der elektro- nischen, eines Nutzers erhalten hat, darf diese für die Versendung von Text- oder Bildmitteilungen an ein Telefon oder an eine Postadresse zu Zwecken der Ber- atung des Nutzers, der Werbung für eigene Angebote und der Marktforschung ver- wenden, es sei denn, dass der Nutzer einer solchen Verwendung widersprochen hat. Die Verwendung der Rufnummer oder Adresse nach Satz 2 ist nur zulässig, wenn der Nutzer bei der Erhebung oder der erstmaligen Speicherung der Ruf- nummer oder Adresse und bei jeder Versendung einer Nachricht an diese Ruf- nummer oder Adresse zu einem der in Satz 1 genannten Zwecke deutlich sichtbar und gut lesbar darauf hingewiesen wird, dass er der Versendung weiterer Nach- richten jederzeit schriftlich oder elektronisch widersprechen kann.“

Der bisherige Absatz 2 wird Absatz 3.

➤ **Datenschutz: Koppelungsverbot (§ 12 Abs. 3 TMG-E sowie Antrag von B90/Die Grünen Nr. 4)**

Es ist zu begrüßen, dass die Bundesregierung in ihrem Entwurf für das TMG das – in seiner Notwendigkeit überhaupt fragliche und in seiner Ausgestaltung zweifelhafte – Koppelungsverbot gegenüber der bisherigen TDG-Regelung jedenfalls nicht verschärft und ein entsprechendes Ansinnen des Agrar- und Verbraucherausschusses des Bundesrates zurückgewiesen hat. Vor diesem Hintergrund sollte auch der Forderung nach einer Verschärfung des Koppelungsverbots im Antrag von Bündnis 90/Die Grünen eine Absage erteilt werden.

Mit Bezug auf Werbemaßnahmen würde das Verbot, eine entsprechende Nutzererklärung in eine Datenschutzeinwilligung zu integrieren, den im vorstehenden Absatz dargelegten europarechtlichen Vorgaben noch weiter zuwiderlaufen. Die Notwendigkeit, eine solche Einwilligung einzuholen, entsteht erst aus der fehlenden Umsetzung der genannten europäischen Regelungen zum Marketing innerhalb bestehender Kundenbeziehungen. Nach diesen Vorgaben soll in bestehenden Kundenbeziehungen (und um solche handelt es sich, wenn eine Anmeldung zu einem Telemediendienst erfolgt) die Möglichkeit zum jederzeitigen opt-out ausreichen, während das ausdrückliche opt-in in diesen Fällen nicht erforderlich ist. Dies ist auch sachgerecht, da es sich hier gerade nicht um die sicher lästigen Fälle einer sog. „Kaltakquise“ handelt, sondern der Nutzer durch seine Anmeldung gerade sein Interesse an dem spezifischen Dienst zum Ausdruck gebracht hat. Die Möglichkeit zum jederzeitigen opt-out schützt ihn dabei hinreichend vor Werbung, die für ihn nicht informativ, sondern nur störend ist.

Ein generelles Koppelungsverbot kann aber auch massive Auswirkungen auf den Verbraucherschutz haben. Denn für eine Reihe wichtiger Sicherheitsmaßnahmen zum Schutz der Nutzer besteht bedauerlicherweise keine gesetzliche Ermächtigung zur Datennutzung. Hierzu gehört einerseits der Einsatz von Sicherheitstechnologien, mit denen – wie etwa auch aus dem Finanzsektor für Kreditkarten oder aus dem TK-Bereich bei Mobilfunkkarten bekannt – ungewöhnliche Nutzungen von Kundenkonten aufgespürt und unterbunden werden können. Nur so können Missbräuche unseres Marktplatzes (etwa durch infolge Phishing gekaperten Mitgliedskonten) frühzeitig entdeckt und Betrugsversuche vereitelt werden. Andererseits fehlt eine klare Ermächtigung zur Kooperation mit der Polizei und der Unterstützung der Ermittlungsarbeit durch Herausgabe von Daten, um kriminelle Geschehnisse im engen Zusammenwirken mit den staatlichen Stellen schnell und effektiv (bevor etwa weitere Nutzerdaten zur Täterverfolgung nicht mehr zur Verfügung stehen) aufklären zu können. Für beide Maßnahmen holt sich eBay mangels gesetzlicher Ermächtigungen eine Einwilligung seiner Nutzer ein. Diese Möglichkeit darf nicht durch ein Koppelungsverbot zunichte gemacht werden, da damit gerade den schwarzen Schafen die Möglichkeit gegeben würde, die bislang sehr effizienten Sicherheitssysteme zu umgehen und anderen Nutzern erhebliche Schäden zuzufügen. Kriminelle in dieser Form zu Straftaten einzuladen, kann nicht im Interesse einer an Verbraucherschutz orientierten Politik sein.

Berlin, den 6. Dezember 2006

Kontakt:

eBay GmbH
Dr. Wolf Osthaus
Leiter Government Relations
Marktplatz 1 - 14532 Europarc Dreilinden
Tel.: 030 / 8019-5314
wolf.osthaus@ebay.de