Spam-Politik
Politisch-rechtliche Bekämpfung unerwünschter Information

Dirk Schmidt

Dezember 2004

Zusammenfassung

Spam ist ein nicht einfach zu fassender Begriff. Unterschiedliche Perspektiven auf die spam-Phänomene, entgegenstehende Interessen und die Historie führen zu unterschiedlichen Problemdarstellungen und schließlich Lösungsvorschlägen für die spam-Bekämpfung. Dieser widmet sich der Beitrag aus politikwissenschaftlicher Sicht, strukturiert, zeigt Akteure, ihre Ziele und Lösungen auf. Komplexer wird die spam-Bekämpfung dadurch, dass sie von Entwicklungen in anderen IT-Bereichen beeinflusst wird, wie auch diese eine Infrastruktur für andere Zielsetzungen - z.B. Lösungen für den Schutz von Verwertungsrechten - bieten kann.

1 Definitionsmacht

SPAM in Großuchstaben ist ein registriertes Warenzeichen der Hormel Food Corporation. SPAM steht für *spiced ham*, übersetzt gewürzter Schinken. Das Fleisch kommt in markanten quaderförmigen, blauen Dosen mit gelbem Schriftzug daher. In einem berühmten Sketch thematisiert die englische Comedy-Truppe *Monty Phython* die monotone, endlos langweilige Ernährung mit SPAM durch endlos langweilige, montone Wiederholungen des Wortes *spam* in einem absurden Restaurant mit absurden Gästen, unter anderen einem Wikinger-Chor. Der Sketch greift dabei auf eine kollektive Erfahrung vieler Briten während des zweiten Weltkrieges zurück, für die SPAM oftmals das einzig verfügbare fleischliche Nahrungsmittel war. Eine einseitige Auswahl, die schließlich zu folgendem Satz im Sketch führt: “But I don’t want any SPAM.“ (zu Deutsch ungefähr: „Aber ich will berhaupt keinen SPAM.“) Diese anwidernde, endlos wiederholende SPAM-Monotonie führte zur der Analogie, die hinter dem Wort Spam steckt - nun in angepasster Orthografie. Spam ist semantisch reduziert eine endlose, sinnentleerte Wiederholung des Immergleichen.

Spam-Phänomene im Internet gibt es nicht nur im Rahmen des Email-Dienstes. Das Wort wurde zunächst in MUDs verwendet und lange Zeit war Spam auch im *usenet* ein Problem. Weitere spam-Phänomene tauchen in Instant-Messenger-Diensten, in Blogs, Suchmaschinen und auch in Mobiltelefonnetzen auf. Als eigentliches Problem stellt sich im Moment der Spam im Email-Dienst dar. Dies war wie angeführt nicht immer so und muss in Zukunft auch nicht so bleiben, so dass vielfach gefordert wird, dass Techniken und Vorschriften gegen Spam nicht nur einen Dienst erfassen sollen, sondern möglichst über die Grenzen von einzelnen Diensten und Medien hinweg wirken sollten. Hier sei ausschließlich Spam im Email-Dienst behandelt.

Dass Spam per Email ein Problem ist, ist aufgrund seines derzeit großen prozentualen Anteils am gesamten Email-Verkehr und der Menge der übertragenen Daten unumstritten, auch wenn verschiedene Schätzungen über das exakte Ausmaß weit auseinandergehen. Ferris Research schätzt die Kosten, die Spam bei amerikanischen Firmen in 2003 verursacht, auf 10 Milliarden US-Dollar[1], 255 Millionen US-Dollar würden allein die Kosten für den Download durch Nicht-Firmen betragen. Für die Bearbeitung einer einzigen Spam-Mail benötige ein Empfänger 4-5 Sekunden. Weltweit werden täglich 12 Milliarden spam-Mails verschickt, wobei das gesamte Email-Volumen auf über 30 Milliarden pro Tag geschätzt wird.[2] Die Zahlen sind schwer zu ermitteln und zu vergleichen, da das individuelle Spam-Aufkommen aufgrund sozialer Kriterien variiert. Das spam-Aufkommen bei privaten Email-Adressen ist so zum Beispiel auch höher als bei beruflich genutzten Email-Adressen.[3] Auch ist die Sicht der Akteure auf Spam verschiedenen: Werden pro Tag und Person durchschnittlich sechs Spam-Mails empfangen, so haben die ISPs mit einem viel größeren Spam-Aufkommen zu kämpfen. Dies umfasst auch alle Spam-Mails, die nicht zugestellt werden konnten, den zugehörigen *error traffic* und auch erfolgreich aus dem Netz gefilterten Spam, den der Endanwender nicht mehr zugestellt bekommt.

Grundsätzlich kann eine formelle und eine inhaltliche Perspektive auf Spam unterschieden werden, aus denen unterschiedliche Definitionen und Lösungen resultieren. Die formelle Perspektive beurteilt eine Mail als Spam idealisiert anhand dem Blick auf eine einzelne Email. Die konstituierenden Elemente einer Email sind dabei der eigentliche Inhalt, der *body*, und der Nachrichtenkopf (*header*) mit Empfängeradresse, dem Betreff, den Absenderangaben und der Information, welchen Weg die Email durchs Internet genommen hat, der *routing information*. Anhand Eigenschaften dieser Elemente soll eine Email als *spam* (Spam) oder *ham*, als Nicht-Spam, iden-

[1] Ferris Research: Research Focus: Spam; http://www.ferris.com/pub/FR-126.html (zuletzt 22.2.2004)

[2] Spamfilterreview.com

[3] Fallows, Deborah: Spam - How It Is Hurting Email and Degrading Life on the Internet; Pew Internet & American Life Project; Washington, D.C./USA 2003; http://www.pewinternet.org/reports/pdfs/PIP_SPAM_Report.pdf (zuletzt 22.2.2004)

tifiziert werden. Oftmals werden diese formellen Kriterien noch zusätzlich um externe Informationen, welche der Mailserver oder Anti-Spam-Dienste liefern, ergänzt, um eine bessere Identifizierung mit mehr Treffern bzw. weniger falschen Treffern (*false positives*) zu erzielen. Die inhaltliche Perspektive sortiert Spam-Mails nach inhaltlichen Kriterien. Ihr Blick ist auf Emails im Vergleich gerichtet. Hierbei zeigt sich sehr schnell, dass es nur wenige Themen gibt, die in Spam vorkommen. Die FTC hat eine Übersicht der 12 Themen ermittelt.[4] Inhalte in Nachrichten und Betreffen erlauben auch ein Filtern nach formellen Kriterien, zumindest nach Phrasen wie „click below“ und „v1agra“. Die inhaltliche Perspektive fragt aber auch nach dem Zustandekommen der zugrundeliegenden Email-Kommunikation, nach Motiven und rechtlichen Grundlagen. Allesamt Kriterien, welche nicht mehr einfach in Software umgesetzt werden können, um den Posteingang eines individuellen Empfängers für sich zu filtern. Die erste Perspektive neigt zur Entwicklung von Filtersoftware und stärkeren formellen Kriterien, die ein effektiveres Filtern erlauben. Die zweite Perspektive richtet sich auch auf die gesellschaftlichen Umstände von Spam, dabei schließt sie Filter und ihre Probleme mit ein.

Der Spam-Begriff ist ein anhand einiger formeller, derzeit softwareverarbeitbarer Kriterien schwierig zu definierender Begriff. Die Reduktion auf „unerwünschte Information“ liefert ein stark subjektives Attribut. Massen-Emails von Absendern, die den Empfängern unbekannt sind, werden zu 92% als Spam bezeichnet[5]. Ist der Absender jedoch eine politische (74%) oder eine karikative Organisation (65%), dann steigt die Akzeptanz deutlich an. Die Akzeptanz von Emails als *ham* variiert aber auch mit dem Typ des Nachrichteninhalts. Pornographie (92%) wird von US-Amerikanern stärker als Spam wahrgenommen als Nachrichten medizinischen, politischen (je 78%) und religösen (76%) Inhalts. Aber auch eine persönliche, individuelle erstellte und zugesandte Email von einer dem Empfänger unbekannten Person - selbst bei nicht-kommerziellem Charakter - wird vielfach (74%) als Spam wahrgenommen. Es ist insgesamt ein großer Unterschied, was subjektiv als Spam - als unerwünschte Information - wahrgenommen wird, und was objektiv - allgemein akzeptiert, als kleinster gemeinsame Menge aller individuellen Definitionen - als Spam definiert wird.

Eine verbreitete Definition[6] besteht darin, die Kriterien unaufgefordert bzw. unangefordert zugesandt, massenhafter Versand und kommerzieller Inhalt zu kombinieren. Als UBE (*unsolicited bulk email*) wird dabei eine massenhaft und unangefordert zugesandte Email bezeichnet. Massenhaft ist ein Kriterium, das auch auf viele bestellte Newsletter und Rundmails zutrifft, wobei die Abgrenzung von „massenhaft“ bereits schwierig ist. UCE (*unsoli-*

[4]Federal Trade Comission: FALSE CLAIMS IN SPAM; 30.4.2003; http:/www.ftc.gov/reports/spam/030429spamreport.pdf (zuletzt 22.2.2004)

[5]siehe Fußnote 3

[6]vgl. Spamhaus, http://www.spamhaus.org

cited commercial email) bezeichnet eine Email, die unangefordert zugesandt wurde und kommerziellen Inhalts ist - also Werbung enthält. Das Kriterium „massenhaft“ taucht hier nicht auf. UCE und UBE können erwünschte und nicht-erwünschte Erscheinungen sein, selbst wenn sie unangefordert zugesandt wurden. Vielleicht will ja nur der nette Computerladen um die Ecke auf ein neues Produkt hinweisen, das dort aufgrund intimer Kenntnisses der IT-Bedürfnisse des Kunden für diesen besonders interessant erscheint, oder ein gute Seele warnt die Netzgemeinschaft vor drohenden gesetzgeberischen Aktionen wieder die Freiheit im Internet. Erst die Kombination der Kriterien, wenn eine Email sowohl UBE, als auch UCE ist, wird nach diesem Ansatz als Spam bezeichnet. Spam ist so folglich eine Email, die ungangefordert, massenhaft versandt wurde und kommerziellen Inhalts ist: “A message is Spam only if it is both Unsolicited *and* bulk.“ [7]

Spam so zu definieren ist eine Möglichkeit. Letzlich ist es wieder nur eine individuelle Perspektive. Unerwünscht zugesandte Emails werden von zahlreichen Nutzern dennoch als unerwünschte Information betrachte, selbst wenn sie nicht massenhaft versandt wurden. Der massenhafte Versand des gleichen Inhalts - wobei keine Quantifizierung von „massenhaft“ vorliegt - kann zudem noch versteckt werden, so dass dies dem Empfänger nicht offensichtlich ist. Politische und religiöse Emails stellen für weitere Nutzer ein ebensolches Ärgernis dar wie Werbe-Emails. Vielfach scheinen Spam-Definitionen Interessen geleitet zu sein. Hierbei sollen bestimmte Formen an UBE bzw. UCE erhalten bleiben. Als Spam werden dann nur die unerwünschten, „bösen“, Emails bezeichnet. Wer die Definition von Spam bestimmt, bestimmt, was bekämpft wird. Wie bei der Umfrage angeführt, genügt vielen Nutzern bereits das Kriterium „unangefordert“, das sowohl in UCE, als auch UBE bereits vorhanden ist. Für diese Nutzer ist Spam dann nicht die Schnittmenge, sondern die Vereinigungsmenge beider Formen.

Aufgrund der wichtigen Bedeutung der Spam-Definition scheint es mir vielversprechender zu sein, Spam als Gattungsbegriff einer Gruppe von Email-Typen - inhaltlich betrachtet - zu setzen. Spam wird hier auf unerwünschte Information reduziert, so dass auch UCE und UE bereits zwei Kategorien von Spam bilden. Die Kategorien sind nicht trennscharf, quasi akademisch, bieten anhand unterschiedlicher Ursachen und Maßnahmen zur Bekämpfung ein gutes Instrument zur Analyse. Schwierig abzugrenzen sind individuell nervende Emails, zum Beispiel eines Freundes, der einen hin und wieder mit

[7] siehe Fußnote 6
Die *Anti Spam Task Force* von *eco* geht einen Schritt weiter, führt die persönliche Empfindung ein und passt die Definition dem EU-Verständnis an: „Eine unverlangt zugesandte Mitteilung (Mail, Messaging, Nachrichtendienst etc.) außerhalb von bestehenden persönlichen oder geschäftlichen Beziehungen, die der Empfänger als unerwünschte Belästigung empfindet, ist Spam.“ in Braun, Dietmar; Kocovski, Jan; Rickert, Thomas; Waldhauser, Dr. Béla: White Paper; eco - Electronic Commerce Forum (Hrsg.); Version 1.00, 21.09.2004; Köln 2004

witzigen Emails belästigt, die andere Nutzer gern empfangen. Die ersten vier Kategorien[8] sind UCE, UBE, „Kettenbriefe und hoaxes“[9] sowie Rufschädigungen[10]. Die weiteren vier Kategorien bezeichne ich insgesamt auch als trojanischen Spam, da sie anderen Zwecken als die Mails der vorherigen Kategorien dienen und nicht für sich stehen, sondern mehr Teil einer weiterreichenden, komplexeren Struktur sind. Die Kategorien sind Viren und Würmer, Trojaner, Phishing und Spamfutter. Letztere bezeichnet Spam, der gar nicht für den Empfänger gedacht ist, sondern für die Instrumente der Spambekämpfung, in der Regel sollen hier zum Beispiel bayesche Filter so durch Spamfutter manipuliert werden, dass andere Spam-Mails passieren können. Phishing ist aufgrund des hohen Anteils an *social engineering* in seinen Inhalten dem *hoax* verwandt, teilt mit dem *hoax* aber nicht die Art der Verbreitung, da hier nicht die Empfänger zum weiterversenden animiert werden.[11] Auch Viren und Würmer, die sich per Email verbreiten, als Spam zu erfassen, rechtfertigt sich, da sie zum einen auch unerwünscht zugesandte Informationen - mit begleitender ASCII-Nachricht oder allein als Binärdatei - darstellen, zum anderen da inzwischen beide Phänomene in der zweiten Jahreshälfte 2003 zusammengewachsen sind. Viren und Würmer werden von Spammern zur Errichtung einer Spamming-Infrastruktur benutzt. Per Viren und Würmern gekaperte Rechner werden zombiegleich als Spam-Versandmaschinen genutzt. Eine Bekämpfung der Verbreitung von Viren - unerwünschten Informationen dieser Kategorien - bekämpft so auch insgesamt die Infrastruktur, also andere Kategorien. Mit dem Hinweis, dass *hoaxes* am schwierigsten mit IT zu bekämpfen sein sollten, da ihr Versandmechanismus über den Nutzer per *social engineering* funktioniert, hier nur Aufklärung wirkt, soll die Darstellung der Kategorien und die unterschiedlichen Arten der Bekämpfung enden. Ein Aktionsplan der alle Kategorien erfasst ist derzeit nicht zu erkennen, wie die Bekämpfung des Spam-Phänomens oft nur eine Kategorie erfasst. Die Kategoriesierung stellt eine Perspektive auf Emails und Email-Spam dar.

[8] Schwartz, Alan & Garfinkel, Simson: Stoppt Spam - kurz und gut; Köln 1999

[9] Ein hoax ist eine Email, die an sich nicht kommerziellen Charakters ist und sich via Techniken des *social engineering* verbreitet, d.h., den Empfänger animiert, sie an weitere Email-Adressen weiterzuleiten. Kettenbriefe sind ähnlich, verbreiten in der Regel Geschäftsschemen der Form *make money fast* (Multi-Level-Marketing).

[10] Rufschädigungen sind im Prinzip Spam, der den Anschein erweckt, von jemandem versendet worden zu sein, um dessen Ruf zu schädigen.

[11] Ich habe bereits eine Form von *phishing* gesehen, ich nenne es *social phishing*, das über eine Internetseite erstellt wird, um sexuelle Vorlieben im Rahmen eines Fragebogens von einem Dritten zu erfragen, der den Fragebogen für eine unterhaltsame Sache wie in Magazinen hält. Ohne dass es der Ausfüllende erfährt, erhält der Urheber der *phishing mail* eine Kopie der eingegeben Daten zugesandt, während der Fragebogen für den Ausfüllenden automatisiert ausgewertet wird. Diese Form von *phishing* ist dann kein UCE. In der Regel scheint Phishing UCE zu sein, allerdings sind die Absenderangaben gefälscht.

2 Adressen

Perspektiven auf Spam betrachten zumeist die fertigen Spam-Emails nach Eingang beim Empfänger bzw. seinem ISP. Inhalte und Sender werden hier genauer untersucht und klassifiziert. Diese Betrachtung erfolgt in einem Sender-Empfänger Modell, bei dem die Kommunikation über eine Nachricht - den Inhalt einer Email - erfolgt. Diese Perspektive des Sender-Empfänger-Modells verdrängt zu leicht, das am Anfang einer Kommunikation via Email der Empfänger steht. Dessen Email-Adressen muss zunächst einmal vorliegen oder generiert werden. Die Erkenntnis um diese Voraussetzung, dem vorliegen einer gültigen Empfängeradresse, führt zu einer Perspektive die sich der Herkunft, der Zweckbindung und Berechtigung zur Nutzung einer Email-Adresse widmet. Eine EU-Studie[12] führt die vier Arten, zugleich Stufen, an, wie eine Email-Adressen in einen Verteiler für - wie auch immer gearteten - Spam geraten kann. Die Stufen sind dabei nach ihrer Akzeptanz durch den Nutzer gegliedert. Spam - wiederum hier die schlimmste, „böse“ Form dieser Systematik - liegt demnach dann vor, wenn die Adressen aus einer unbekannten Quelle stammen, insbesondere nicht vom Einverständnis der Nutzer zur Zusendung von Emails ausgegangen werden kann. Die nächste Stufe wird als *opt-out* bezeichnet. Ein Einverständnis zur Nutzung der Email-Adressen liegt auch hier nicht vor, jedoch weisen die Spam-Mails hier darauf hin, was getan werden muss, um künftig keine weiteren Spam-Mails, zumindest vom Urheber der jeweils betrachteten Email, mehr zu erhalten. Der Empfänger hat also die Möglichkeit zum *opt-out* - daher stammt der Name. Der große Fortschritt zur nächsten Stufe dieser Kategorisierung besteht nun im Übergang von *opt-out* zu *opt-in*. Bei *opt-in* hat der Nutzer der Zusendung zugestimmt, in dem er sie zum Beispiel selber für einen Newsletter angemeldet hat. Diese Form der Registrierung für die Zusendung von Emails bietet jedoch einige Probleme: Nicht-Berechtigte können die Email-Adressen anderer registrieren, um entweder die Inhaber der Adresse zu schädigen, da sie unerwünschte Informationen erhalten, oder um die Absender zu schädigen, da die Empfänger irrtümlich glauben Spam von ihnen zu erhalten. Die Idealform dieser Systematik besteht im sogenannten *confirmed opt-in* - auch *double opt-in* genannt -, bei dem auf die Registrierung einer Email-Adresse noch eine Bestätigung über eine erste zugesandte Email nötig ist. Die dafür nötige Email kann natürlich immer noch als Belästigung, als unerwünschte Information betrachtet werden, generiert aber keine weiteren Spam-Mails, falls nicht entsprechend geantwortet wird. Diese Systematik veranschauchlicht hervorragend die unterschiedlichen Ansätze, die aufgrund unterschiedlicher Realisierung des Datenschutzes in bezug auf Email-Adressen gängig sind.

[12] Gauthronet, Serge und Dourard, Etienne: Unsolicited Commercial Communications and Data Protetion; Commission of the European Communities (Hrsg.); http://europa.eu.int/comm/internal_market/privacy/docs/studies/spamsum_de.pdf (zuletzt 22.2.2004)

Exemplarische Vertreter mit unterschiedlichem Datenschutzniveau sind die Europäische Union (EU) und die Vereinigten Staaten von Amerika (USA). In der Europäischen Union ist Datenschutz ein Grundrecht, das entweder als Ausfluss der Persönlichkeitsrechte angesehen wird (GG, BGB) oder explizit benannt wird - vgl. EMRK und EU-Grundrechtecharta. In den USA existiert kein allgemeines Datenschutzrecht, zumindest nicht im Verhältnis zwischen Privaten, wo es Teil vertraglicher Ausgestaltung ist.

Die Spam betreffenden Regelungen der EU finden sich in der EU-Richtlinie 2002/58/EG zur Telekommunikation. Die Richtlinie hat eine Vorgeschichte: Sie löste die alte Richtlinie 1997/77/EG ab, basiert auf Regelungen der Datenschutzrichtlinie 1995/46/EG und klärt einen scheinbaren opt-out-Ansatz der Fernabsatzrichtlinie 1997/7/EG. Die EU-Datenschutzrichtlinie etablierte den Datenschutz für alle EU-Mitgliedsstaaten, vorher war der Datenschutz in der EU wenn überhaupt, dann nicht einheitlich geregelt. Im europäischen Wirtschaftsraum gilt nun das gleiche hohe Datenschutzniveau und Daten werden EU-weit gleich behandelt, können ohne Verlust des Schutzniveaus und der Zweckbindung im europäischen Wirtschaftsraum und in einige Länder mehr exportiert werden, ohne das das Grundrecht bzw. abgeleitete Grundrecht auf informationelle Selbstbestimmung beeinträchtigt wird. Zu diesen Daten zählen auch die Email-Adressen natürlicher Personen. Die Ausgestaltung betreffend juristischer Personen ist den nationalen Gesetzgebern überlassen. Auch die Fernabsatzrichtlinie, die Unternehmen das Beschicken von Kunden mit Werbung gestattet, bis dass diese widersprechen, änderte daran nichts. Eine Email kann nicht legitim versandt werden, wenn die Adresse unter Verstoß gegen den Datenschutz erfasst, gespeichert und verwendet wurde.

Die Telekommunikation-Richtlinie dehnt das opt-in-Verfahren, das bisher für Faxe und automatisierte Telefonanrufe galt, auf den Bereich des Email-Verkehrs aus, in dem es drei einfache Prinzipien für unangefordert zugesandte kommerzielle Emails (UCE) - Werbung - aufstellt. Die erste Regel (Artikel 12) schreibt vor, dass die Mitgliedsstaaten verpflichtet sind, ein opt-in-Verfahren zu erlassen. Ein opt-in der Empfänger hinsichtlich des Empfangs von UCE ist zwingend erforderlich, jedoch (Artikel 13(2)) gibt es eine Ausnahme davon, die es gestattet, Emails an Personen zu senden, mit denen bereits ein Kundenverhältnis besteht. Diese Ausnahme ist jedoch streng eingeschränkt auf ähnliche Produkte und gilt ausschließlich für die gleiche juristische Person, also nur für die Firma, mit der der Kunde auch wirklich in ein Kundenverhältnis getreten ist. Das zweite Prinzip verbietet es, die Identität des Absenders zu verbergen - ähnliches findet sich bereits in der Fernabsatzrichtlinie. Das dritte Prinzip schreibt zwingend eine gültige Rückantwortadresse vor, bei der der Empfänger der Email sich kostenfrei und auf einfache Weise sich eines opt-outs von weiteren Emails bedienen darf. Ein *remove request* muss somit vorhanden sein. Innerhalb der EU kommt somit nur ein *permission based marketing* in Frage, wobei

dem Datenschutz genüge getan ist, da die zulässige Zusendung von Emails an die Zustimmung des Inhabers gebunden ist. Diese Zustimmung wird für den Fall unterstellt, dass eine Kundenbeziehung vorliegt und dass die Email darauf wie angeführt inhaltlich bezogen ist. Dies gilt EU-weit jedoch nur für Emails natürlicher Personen. Da für juristische Personen Grundrechte nur bedingt gelten, ist es – wie bereits angeführt – den nationalen Gesetzgebern freigestellt, dies anders zu regeln, wie sie auch für künftige Formen elektronischer Werbung eine Wahl zwischen einem opt-in- und einem opt-out-Modell haben.

Eine deutsche Besonderheit ist das Verbot von Spam, von unangefordert zugesandten kommerziellen Emails ohne vorliegende Kundenbeziehung, nach dem Gesetz gegen den unlauteren Wettbewerb (UWG). Die EU-Richtlinien schlagen sich auch in einer Änderung des UWG zum 1.1.2004 nieder. Historisch lässt sich die durch die Entwicklung der unerwünschten Werbung anhand anderer Medien erklären. Dass Spamming unlauterer Wettbewerb ist, verdrängt nicht die Argumente, die aus dem Recht auf informationelle Selbstbestimmung abgeleitet sind. Sie greifen subsidiär, wenn die Argumentation des unlauteren Wettbewerbs nicht mehr greift, so zum Bespiel im Bereich der politischen Werbung. Politische Werbung ist daher der kommerziellen Werbung gleichgestellt[13], also verboten, da sie einen Eingriff in die Persönlichkeitsrechte des Empfängers darstellt, einem Grundrecht das - so zumindest die derzeit vorliegenden richterliche Urteile - auch nicht durch das Parteienprivileg des Grundgesetzes eingeschränkt wird. Das UWG hat den Vorteil hinsichtlich der Spam-Bekämpfung, dass es Konkurrenten und Verbraucherschutzverbänden ein Klagerecht einräumt, während sonst die Verfolgung der Einschränkung des individuellen Personlichkeitsrechts individueller Initiative bedarf, sofern es nicht so gravierend ist, dass der Staat einschreiten muss. Ein staatliche Schutzgarantie für mit Spam überflutete Personen besteht nicht, aber abgeleitet werden könnte doch ein Anspruch auf staatliche Maßnahmen, etwas gegen Spam zu tun, wenn so viele Bürger betroffen sind. Wobei Regierung und Gesetzgeber die weitestgehende Freiheit der Ausgestaltung zukommt, so dass dieser Gedankengang hier nicht weiterverfolgt werden braucht. Ergänzt sei zuletzt, dass auch das UWG den ISPs kein vielfach gefordertes Klagerechtrecht einräumt.

Die USA kennen nach dem *CAN SPAM act of 2003* kein opt-in-Modell, sondern nur das opt-out-Modell. Absender von unangefordert zugesandten, kommerziellen Emails haben in der Email eine Postanschrift und einen *remove request* anzugeben. Weiterhin ist hat der Absender über eine funktionierende Email-Adresse zu verfügen, welche ggf. bereits für den *remove request* verwendet wird. Damit wird das einfache elektronische Antworten für die Empfänger gewährleistet und auch, dass ein irreleitender, falscher Absender angegeben wird. Der *remove request* eines Nutzers ist zwingend durch

[13] siehe Urteil AG Rostock, 28.1.2003

den Versender zu befolgen, wobei das Bundesgesetz Formalien wie die hierzu maximal zulässige Bearbeitungszeit regelt. Zuletzt haben diese UCEs sich inhaltlich eindeutig als Werbung erkennenzugeben. Die Gemeinsamkeiten der EU-Richtlinien und des US-Gesetzes sind die Verbote des Verbergens bzw. Fälschens der Absenderangaben, des Fehlens einer Rückantwortadresse und eines *remove request* sowie die eindeutige Identifizierbarkeit als Werbung. Diese Vorschriften stärken gesetzlich die formellen Elemente einer Email, da Manipulationen dieser Angaben und die Täuschung darüber, dass es sich um Werbung handelt, diese gleich als nicht-legitime Emails - als Spam - einstufen. Dem amerikanischen opt-out-Modell steht jedoch das europäische opt-in-Modell gegenüber. UCEs können in den USA so lange legal zugesandt werden, wie der Empfänger keinen Einwand über den *remove request* erhebt. Also zumindest einmal ist eine UCE an einen Empfänger zulässig. Anders aufgestellt ist der EU-Ansatz, bei dem bereits eine erste UCE ohne Zustimmung des Empfängers unzulässig ist, sofern nicht die Ausnahme der Kundenbeziehung vorliegt oder der Empfänger gegebenenfalls eine juristische Person ist, für die eventuell nur ein opt-out-Verfahren gilt. Zumindest für natürliche Personen stehen sich die Regelungen entgegen. Konkret darf in der EU somit keine einzige Email an im Internet per Software oder Hand auf irgendwelchen beliebigen Seiten gesammelter Email-Adressen verschickt werden, was in den USA zumindest für eine erste Email zulässig ist. Aufgrund der EU-Datenschutzrichtlinie wäre bereits das hierfür benötigte Erfassen und elektronische Speichern der Email-Adresse in einer Datenbank nicht zulässig. Das Fehlen eines allgemeinen Datenschutzrechtes in den USA hingegen lässt das Sammeln (*harvesting*) und Speichern von Emails im Internet zu. Dass dies die Grundlage für Spamming ist, hat auch der US-Kongress erkannt und daher im CAN SPAM act die hierfür benötigte Software - eine Form sogenannter Spamware - verboten, was zumindest das automatisierte Sammeln von Email-Adressen etwas erschwert. Aufgrund des Fehlens eines allgemeinen Datenschutzrechts hat der US-Gesetzgeber zu diesem Vehikel gegriffen. Diese Spamware ist in der EU nicht verboten, jedoch ihr Einsatz, wenn er zu einer Datenbank führt, der Daten - also Email-Adressen - erfasst, bei denen kein Einverständnis der Inhaber (natürliche Personen) vorliegt. Legitime Nutzungen der Software sind vorstellbar, zum Beispiel das Sammeln von Email-Adressen im Intranet einer Firma. Dass die hierfür benötigte Software eine legitime im Sinne des CAN SPAM act ist, dürfte die Abgrenzung von *harvesting tools* unmöglich machen, da innerhalb eines Intranets und des Internet die gleiche Software eingesetzt werden kann. Kurz gefasst heisst das, dass Spamware zwar verboten ist, die gleiche Software aber auch immer legale Nutzungen kennt. Es kommt daher auf den Zweck an, für das diese Instrumente eingesetzt werden und nicht auf das Instrument selber.

Insgesamt führt das Fehlen eines allgemeinen Datenschutzrechts bezogen auf das Verhältnis zwischen privaten Akteuren in den USA zu einer

stärken Berücksichtigung wirtschaftlicher Interessen. So ist fiktiv eine erste Email zulässig - Spamming bis zum opt-out. Um dies zu mildern, fordert der CAN SPAM act aber nicht nur ein opt-out-Verfahren, sondern spricht sich für ein globales opt-out-Verfahren aus. Global bedeutet dabei, dass die Angabe, dass der Nutzer überhaupt keine UCE wünsche an einer einzigen zentralen Stelle geäußert dazu führe, dass er überhaupt keine UCEs mehr erhalte. Das opt-out bei jedem einzelnem Versender wird so durch ein globales vorweggenommen. Im CAN SPAM act hat der US-Kongress die *federal trade commission* (FTC) angewiesen, einen Bericht zu verfassen, inwiefern ein dafür nötiges Register, vergleichbar der Robinsonliste des Deutschen Direkmarketingverbandes (DDV) bezüglich Werbung per Post, realisierbar ist. Hierzu hat die FTC im Juni 2004 einen Bericht[14] vorgelegt, der ausführt, dass ein derartiges zentrales Register Spam nicht bekämpfen würde, da es Spammern ermöglichen würde, die enthaltenen Adressen für Spamming zu übernehmen. Dies würde das spam-Problem weiter verschlimmern. Die FTC ist davon überzeugt, dass ein Do-Not-Spam-Register nur funktionieren kann, wenn das formelle Kriterium der Email-Adresse gestärkt würde, wenn also Email-Adressen nicht mehr verborgen oder verfälscht werden können. Die Kommission (FTC) spricht sich daher für eine weitere Verbreitung von techischen Lösungen zur Authentifizierung von Absendern aus.

In der vorliegenden Form wird ein opt-out-Verfahren durch ein opt-in-Verfahren in einem grenzlosen Internet ohne Grenzkontrollen zwischen den Bereichen des opt-in- und opt-out-Gebietes nicht gestört. Die Mails aus dem opt-in-Gebiet erreichen die Empfänger nur wenn deren Zustimmung vorliegt und enthalten auch den geforderten *remove request*. die übrigen Mails sind in der Regel Spam. Umgekehrt gilt dies für UCEs aus dem opt-out-Gebiet an Empfänger im opt-in-Gebiet nicht. Zwar enthalten diese UCEs auch den für kommerzielle Emails nötigen *remove request*, aber dies genügt nicht, da die Zusendung bereits unterbleiben muss, wenn keine Zustimmung und keine Kundenbeziehung zwischen Sender und Empfänger besteht. Problematisch ist bereits, dass in der EU bereits das Ernten (*harvesting*) von Email-Adressen und Speichern in einer Datenbank nur mit Zustimmung zulässig ist, also in der Regel überhaupt nicht zulässig ist. Die gleichen Adressen aus den gleichen Adressräumen des Internets, ebenso wie das zufällige generieren von Email-Adressen und schließlich das Anlegen entsprechender Datenbanken ist in den USA hingegen erlaubt. Im Endeffekt führt dies dazu, dass auch nur das opt-out-Modell für den Bereich der EU gilt. Verstöße gegen das opt-out-Modell können dabei grenzüberschreitend kaum geahndet werden. Es handelt sich um komplexe Verfahren mit allen Schwierigkeiten Prozesse im Ausland zu verfolgen oder entsprechende zivil- oder strafrechtliche Ansprüche grenzüberschreitend wahrzunehmen. Entwicklungen auf diesem

[14]FTC 2004: National Do Not Email Registry - A Report to Congress; Washington, D.C/USA, 2004

Gebiet beeinflussen auch die Spam-Bekämpfung.

Opt-in-Verfahren und opt-out-Verfahren sind jedoch miteinander vereinbar, zumindest wenn das Modell eines globalen opt-out-Verfahrens verwendet wird. Globales opt-out bezeichnet in Ergänzung des oben angeführten opt-out-Modells, dass der Inhaber einer Email-Adresse oder einer Internet-Domain diese global vom Erhalt von UCEs abmelden kann. Die Anmeldung an einem 'do not spam'-Register bewirkt bei entsprechender, gesetzlich sanktionierter Berücksichtigung durch die Versender, dass künftig keine UCEs mehr an entsprechende Email-Adressen bzw. *domains* gehen. Insbesondere die Registrierung ganzer *domains* könnte eine Lösung darstellen, wie auch eine Zwangsregistrierung europäischer Email-Adressen an einem derartigen Register durch europäische ISPs. Ein derartiges 'do not spam'-Register zu untersuchen, hatte der US-Kongress die FTC im Rahmen des CAN SPAM act beauftragt. Der Auftrag erfolgte jedoch in Hinsicht auf den Nutzen und die Funktionsfähigkeit eines derartigen Registers, nicht offiziell in Hinblick auf eine Berücksichtigung europäischer Interessen. Wie oben angeführt, kommt der Bericht zu dem Schluss, dass ein derartiges Register nicht funktioniert, wenn Emails - genauer Email-Adressen - nicht weitgehend (*widespread*) authentifiziert werden. Authentifizierung ist für die FTC eine Voraussetzung zum Funktionieren eines entsprechenden Registers. Somit ist ein derartiges Register kein Ausweg, um ein Authentifizierung der Absender zu verhindern, da es diese ebenso benötigt. Ein derartiges Register könnte jedoch auch den Interessen sämtlicher europäischer ISPs, Inhaber von Email-Adressen und -Domains dienen. Die Konstellation ist aber einseitig: Die EU benötigen zur Durchsetzung eines funktionierenden opt-in-Verfahrens die Kooperation der USA. Umgekehrt ist dies nich so. Dennoch dürfte auch für die USA eine Kooperation mit der EU, eine weltweite Kooperation, Vorteile bieten, da dies zumindest das befürchtete Ausweichen der Spammer in weitere Staaten hinreichend berücksichtigt. Hinsichtlich Verhandlungen über die Implementierung von Verfahren, wie zum Beispiel einem globalen 'do not email'-Register, ist das derzeitige Scheitern eines us-amerikanischen Alleinganges nicht das Schlechteste, da es ermöglicht über Verhandlungen noch Interessen weiterer Staaten an einem derartigen Verfahren zu berücksichtigen. In einem grenzenlosen Internet dürfte die Art und Weise der Berücksichtigung der Email-Adressen von Inhabern aus weiteren Staaten eine grundlegende Fragestellung sein, die in internationalem Rahmen verhandelt werden müsste. Gespräche über Spam im internationalen Rahmen finden sich derzeit im Rahmen der OECD und ITU (*International Telecommunication Unit* der UN).

Wenn hier stellvertretend EU und USA angeführt werden, dann daher, weil sich die grundlegende Problematik zwischen opt-in und globalem opt-out stellvertretend an ihnen exemplarisch zeigen lassen. Zudem handelt es sich um die wichtigsten Vertreter. Die übrigen Staaten lassen sich soweit sie Vorschriften hinsichtlich Spam erlassen nach beiden Kategorien sortie-

ren. EU-Richtlinien und CAN SPAM act etablierten hinsichtlich beider Regime zudem erste Vorschriften explizit für Spam, die im Anschluss an vorangehende Experimente der Gliedstaaten erlassen wurden. Diese Vorschriften werden in den kommenden Jahren aber einer Evaluation und Revision bedürfen. Der CAN SPAM act war bereits vor seinem Erlass kritisiert worden, u.a. natürlich, da er nur das „Spammen“ regle (“With this act you CAN SPAM!“). Die Umsetzung der EU-Richtlinien in nationales Recht, insbesondere von 2002/58/EG, hat zu sehr unterschiedlichen Lösungen geführt, so sind die Kompetenzen der Spam-Bekämpfung bei unterschiedlichen Institutionen angesiedelt - mal gehört es zum Bereich der nationalen Telekommunikationsregulierungsbehöre, mal zum Verbraucherschutz, mal zum Datenschutz -, mal ist ein Verstoss gegen die Regelungen sehr günstig, kostet wenige Hundert Euro, und mal ist es sehr teuer, kostet mehrere Zehntausend Euro. Für die Jahre 2005/06 kann daher in den USA und der EU mit verstärkten gesetzgeberischen Maßnahmen gerechnet werden.[15]

3 Akteure

Im Februar und im September 2004 hat die OECD je einen *workshop* zu Spam in Brüssel und in Korea durchgeführt. Hier haben Regierungsvertreter in verschiedenen Foren sich über Fragen der Bekämpfung von *open relays* und der Authentifizierung ausgetauscht. Ein Ergebnis ist das Projekt der Erstellung eines *Anti-Spam Toolkits*, das Instrumente zur Verfolgung von Spammern an die Hand geben soll, ein Projekt dass sich auch bei Akteuren auf nationalstaatlicher Ebene findet. Außer Gesprächen hat es bisher keine von der OECD ausgehenden Aktionen gegeben. Die OECD scheint sich gerade in der Phase der Informationssammlung und Abstimmung zu befinden[16]. Ebenso wie die OECD verfährt die ITU, eine Organisation im Umfeld der Vereinten Nationen. Erklärtes Ziel der ITU ist es die internationale Kooperation - bilateral und multilateral - bei der Spam-Bekämpfung kurz- und langfristig zu fördern. Die Internetseite der ITU enthält eine Übersicht zu aktuellen Konferenzen und *workshops* zur Spambekämpfung.[17] Bisher

[15]Ein Beschluss des EU-Rates von Anfang Dezember 2004 (9.12.2004) scheint dies zu bestätigen. Er kritisiert die unterschiedliche Handhabung in den EU-Mitgliedsstaaten, zieht die Evaluation der Richtline 2002/58/EG vor und sieht vor, Gemeinschaftsmittel für die Entwicklung von Anti-Spam-Techniken zu verwenden. Herausgelöst aus dem Bereich der IT-Sicherheit, scheint mir dies das erste mal zu sein, dass staatliche Mittel für die Erforschung und Entwicklung von Anti-Spam-Software verwendet werden, wenn der Ansatz nicht zu einem weiteren Anti-Spam-Toolkit führt.

[16]So fand nach Kenntnissen des Autors zum Beispiel Anfang Dezember 2004 ein Treffen zwischen Vertretern der OECD und des Verbandes der Deutschen Internetwirtschaft - eco - statt, wo letzterer seine Ziele und Maßnahmen vorstellte.

[17]Zum letzten Quartal 2004 finden sich da Veranstaltungen an folgenden Orten: Kyoto/Japan (02/2005), Brüssel/Belgien (EU-Kommission, 11/2004), Washingon, D.C./USA (u.a. FTC, 11/2004), London/UK (internationale Beteiligung, 10/2004); auch in Brasilien

nur aus Internetforen bekannt, treten inzwischen verstärkt auch Diskussion über Möglichkeiten und Sinn staatlicher Regulierungen im Vergleich zu einer Selbstregulierung der am Internet Teilnehmenden statt. Dem Thema Regulierung versus Selbstregulierung widmete sich zum Beispiel ein Panel beim OECD *workshop* in Korea. Die Bearbeitung auf internationaler Ebene findet im Rahmen von Regierungsorganisationen statt, ist jedoch über diese rückgekoppelt an Akteure auf nationaler Ebene. Diese Rückkoppelung scheint mir jedoch allein zu Wirtschaftsverbänden zu existieren. Software-Hersteller, Anti-Spam-Aktivisten, Verbraucherschutzverbände scheinen unterrepräsentiert zu sein, Direktmarketingverbände finden sich oftmals im Rahmen ihrer Kooperation mit Verbänden der Internetwirtschaft. Ein internationale Kooperation dieser Akteure findet sich nicht. Gegensätzlich so die Positionen des Deutschen Direktmarkting Verbandes (DDV) und der us-amerikanischen Direct Marketing Association (DMA). Während die DDV auf Kooperation setzt - auch im Interesse, ihre legitime Emails nicht als *false positives* gefiltert zu bekommen -, hat sich die DMA Lobbyarbeit wider ein Verbot von Spamming zum Ziel gesetzt. Das Kalkül dahinter ist, dass das Verbot von Spamming den Druck auf Verbot derzeit noch legitimer Werbeformen erhöhen würde; hier muss wieder berücksichtig werden, das Spam unterschiedlich definiert wird. Der Spam-Bekämpfung auf nationaler Ebene über die Implementation von Verfahren und Änderungen am Code - der Software des Internets - sind Grenzen gesetzt, die aufgrund staatlicher bzw. regimebezogener territorialer Grenzen existieren. Aus dem Ausland eintreffender Spam kann so kaum bearbeitet werden. Die Kooperationsvereinbarung zwischen DDV und dem Verband der Deutschen Internetwirtschaft *eco*, die auf dem 2. Deutschen Anti-Spam-Kongress im September 2004 unterzeichnet wurde, kennt daher auch eine Ausstiegsklausel für den Fall, dass sich das entwickelte Positivlistenprojekt als unwirksam herausstellt. [18] Nachfolgend seien einige ausgewählte Projekte der Spam-Bekämpfung aufgeführt:

- *Sender Permitted From (SPF).* Dieses von AOL im Januar 2004 vorgestellte Verfahren setzt auf eine Modifikation des Code des *domain name service* (DNS). Die IP-Adresse, von der eine Email empfangen wird, ist derzeit das einzige formelle Element einer Email, dass nicht verfälscht werden kann. Ein *reverse lookup* im *domain name server* erlaubt zu einer IP-Adressen den - genau gesagt einen - *domain name* zu erhalten. Hier kann nun geprüft werden, ob die *domain* der angegebe-

und China hat es bereits Konferenzen gegeben. Für den nächsten WSIS (*World Summit on the Information Society*) steht Spam ganz oben auf der Agenda. Der EU-Rat hat den EU-Mitgliedsstaatenim Dezember 2004 empfohlen sich an internationalen Aktivitäten zu beteiligen.

[18] Die Wirksamkeit ist wirklich fraglich, wenn 80% des deutschen Spam wirklich aus den USA stammen. Wirksamkeit wäre dann mehr auf den Schutz der legitimen Versender kommerzieller Emails gerichtet. Benötigt würde ein derartiges Projekt auf internationaler Ebene - ähnlich einem staatlich implementierten 'do not email'-Register.

nen Email-Adresse überhaupt zu den IP-Adresse gehört. Leider ist das insgesamt etwas komplexer, da unter der selben IP-Adresse oft mehrere *domains* zu finden sind oder mehrere System ein und denselben Mailserver nutzen. Dies Problem löst nun SPF, welches die zusätzlichen Angaben definiert, damit ein Serveradministrator angeben kann, welche *domains* berechtigt sind, über einen Mailserver Email zu versenden. Kurz gesagt, kann bei der Implementierung durch den Empfänger einer Email oder seinen ISP geprüft werden, ob die anlieferende IP-Adresse berechtigt ist, Emails von der angegebenen *domain* - dem Teil hinter dem @-Zeichen - zu liefern.

Das Verfahren ist eine Art von Authentifizierung, allerdings werden nicht Nutzer authentifiziert, sondern Server. Allerdings täuscht der Begriff „Authentifizierung“, da es sich nur um eine einseitge handelt, denn es ist nur sicher gestellt, dass der Systemadministrator - der Inhaber des Servers - es gestattet, Emails von dieser *domain* zu versenden, nicht sichergestellt ist, ob der Inhaber des *domain name* gestattet, dass Emails in seinem Namen über diesen Server versendet werden. Einfacher, anders gesagt: Ein Versender kann einfach seine Absenderangaben verändern, nicht aber so einfach die versendende IP-Adresse. Der Schutz ist nicht lückenlos, SPF würde aber die Bekämpfung einiger Spamming-Techniken zum Verbergen und Verfälschen der Absenderangaben bekämpfen. Das SPF-Verfahren ist zudem ein freies Verfahren – *open source* –, was sich auch darauf bezieht, dass keine Urheberrechte oder Softwarepatente eine Verbreitung beeinträchtigen-

- *Sender ID / Caller ID.* Die erwähnten Verwertungsrechte sind gerade das Problem bei einer Implementierung des Sender-ID-Verfahren, für das sich die Firma Microsoft, die es entwickelt hat, Patente gesichert hat. Im Prinzip funktionieren Sender ID und das *Sender Policy Framework* ebenso über zusätzliche DNS-Einträge, die definieren, welche *domains* von einer IP-Adresse berechtigt sind, Emails zu versenden. Diese DNS-Einträge können weltweit von anderen Servern abgerufen werden.

  Gegenüber Verfahren, die eine Authentifizierung der Nutzer erforderlich machen, haben *domain name*-basierende Verfahren den Vorteil, dass diese Authentifizierung in zwei Schritten erfolgt: Die Server authentifizieren sich weitgehend untereinander, jeder Betreiber muss dann sicherstellen, dass aber auch nicht jeder – jeder Spammer – Emails über diesen Server versenden kann. Dies macht in der Regel ein Authentifizierung der Nutzer am Server notwendig. Es handelt sich um ein zweistufiges Vertrauensmodell. AOL lehnt Caller ID nicht aufgrund der Technologie oder Patente ab, sondern weil der Konzern befürchtet, dass die *open source*-Szene es ablehnen wird.

- *Staatliche Sanktionierung.* Zivil- und Strafrechtliche Maßnahmen stellen eine Möglichkeit dar, Spamming über das Rechtssystem[19]zu sanktionieren; hierzu gehört auch die Gewinnabschöpfung. Spektakulär ist aktuell die Verurteilung eines amerikanischen Spammers zu neun Jahren Haft in Virginia, jedoch muss diese Sensation ggf. relativiert werden, da eine noch ausstehende richterliche Anordnung diesen *jury*-Spruch im Strafmaß verringern kann.

  Ein strafrechtliche Sanktionierung von Spamming ist in Deutschland derzeit nicht gegeben. Indirekt kann es ggf. verfolgt werden, wenn für das Spamming Manipulationen an fremden Rechnern erforderlich waren, die nach den geltenden Gesetzen gegen Computersabotage etc. bereits strafbar sind. Der verworfene Entwurf (Frühjahr 2004) eines Anti-Spam-Bundesgesetzes der rot-grünen Koalition soll eine strafrechtliche Sanktionen enthalten haben. Etwas milder äußerte sich die CDU, die Spamming als Ordnungswidrigkeit verfolgt sehen wollte.[20] Das Kalkül dahinter war, dass Bußgelder für Spamming dann so einfach per behördlicher Anweisung und ohne komplette Gerichtsverfahren verhängt werden könnten. Erst beim Widerspruch des vermeintlichen Spammers wäre ein entsprechendes Verfahren ggf. nötig. Jeder, der mal ein Knöllchen bekommen hat, kennt das. Ziel ist es vor allem, durch entsprechende Bußgelder die Ökonomie des Spammens zu zerstören. Diese Wirkung gilt analog für Haftstrafen. Es verbleiben jedoch die Schwierigkeiten der Identifizierung der Spammer und der Verfolgung strafrechtlicher und zivilrechtlicher Ansprüche über Territorialgrenzen hinweg.

- *Anti-Spam-Toolkit.* Ein derartiges Toolkit ist weniger eine Software als vielmehr eine Handlungsanleitung für Regierungen, Regulierer oder ISPs. Es stellt Informationen und praktische Anleitungen zur Verfügung. Die OECD hat ein derartiges Projekt hinsichtlich der Beratung von Regierungen gestartet. Zukünftig sollen für das Toolkit auch Programme zur „Erziehung“ der Nutzer entwickelt und eine Übersicht der Lösungsansätze ergänzt werden.

Die Beispiele vervollständigen das Bild, das zeigt, dass alle politischen Regulierungselemente im Bereiche der Spam-Politik zur Verfügung stehen und zumindest diskutiert werden. Zum einen können Sanktionen erlassen werden, und zum anderen Aufklärung der in irgendeiner Form Betroffenen zwecks Verhaltens- oder Einstellungsveränderung (Normen) betrieben werden. Weiterhin können Marktmechanismen etabliert oder verändert werden,

[19]Im Sinne von Selbstregulierung könnte etwas derartiges auch über Verfahren wie Microsofts Bonded Sender erfolgen, wobei in einem solchen Verfahren auch gute Verdienstmöglichkeiten zu finden sind.

[20]vgl. Bundestagsdrucksache 15/2655

was hier nicht analysiert wird. Hingewiesen sei nur auf die Konkurrenz der Email-ISPs (GMX, AOL, Hotmail, web.de etc.), die mit ihrer Anti-Spam-Technologie Kunden umwerben und die Auswirkungen von ggf. einzuführenden Bußgeldern auf die Ökonomie des Spam. Eine große Bedeutung kommt dem Instrument der Veränderung von dem vor, was der amerikanische Autor Lawrence Lessig *Code* nennt. Veränderungen bzw. Ergänzungen der Software des Internets zielen dabei derzeit vordringlich auf die Implemenation von Authentifizierungsmechanismen. Noch haben Staaten und Regime nicht begonnen, sich hier für eine Lösung stark zu machen. Da alle Regulierungsinstrumente in ihrer Leistung beschränkt scheinen, spricht viel für einen multi-dimensionalen Ansatz.

4 Nebeneffekte

Auch wenn viele - technische und rechtliche - Maßnahmen zur Lösung des Spam-Problems diskutiert werden, so scheinen die Überlegungen hinsichtlich einer Technikfolgenabschätzung nicht so weit gediehen zu sein. Diese sollten verstärkt diskutiert werden. Verschiedene Lösungen für unterschiedliche Problemstellungen können sich gegenseitig beeinflussen. Eine Änderung im *domain names service* stellt so eine Lösung für die Spam-Bekämpfung vor. Hier wird ein Vertrauensmodell etabliert, dass der Spam-Bekämpfung dient. Es sei darauf hingewiesen, dass dieses Vertrauensmodell, wenn es erst elaboriert genug ist, weiteren Interessen dienen kann.[23] Eine erfolgreiche Spam-Bekämpfung über die Authentifizierung jeglicher Email eines jeden Benutzers würde die Möglichkeiten anonymer Emails oder Emails unter Pseudonymen verringern, die die derzeit existieren, wenn sie nicht sogar vollständig verschwinden würden. Auch könnten für die Spam-Bekämpfung entwickelte Authentifizierungsverfahren und Vertrauensmodelle für *trusted systems*, *digital rights management*-Systeme (DRM-Systeme) verwendet werden. Die Entwicklungen dieser Technologie bieten aber auch viele Möglichkeiten Spam zu bekämpfen. So vermute ich bei einem etablierten DRM-System genug Möglichkeiten für ein spam-freies Email-System. Technologien, die es ermöglichen die Verwendung von Dateien auf einen Rechner zu beschränken, wofür dieser eindeutig identifizierbar sein muss, dürften diese Identifizierung auch für andere Lösungen zur Verfügung stellen können, so zum Beispiel zur Identifizierung des Absenders. Ein Zwischenschritt besteht darin, anhand von etablierten Verfahren - Vertrauensmodellen - zumindest die Identifizierung von *ham* zu verbessern. Im Zusammenhang zur Diskussionen über Identitätsmanagement entstand folgender Vor-

[23] Durchgedacht werden sollten einmal die Möglichkeiten für die Spam-Filterung in Folge der flächendeckenden Einführung digitaler Signaturen. Welchen Beitrag würden Ausweisdokumente mit Signaturen bieten, wenn diese zumindest in den wichtigsten Industrienationen verbreitet wären?

schlag eines Gedankenspiels: Wie steht es um einen Spam-Filter, der bereits beim geringsten Verdacht, dass es sich um eine Spam-Mail handelt, diese löscht, aber über eine *whitelist* verfügt, die auf mindestens 50 positiven Bewertungen bei eBay oder alternativ auf der Erfassung der Adressdaten bei der SCHUFA basiert?

5 Fazit

Anstatt eine Zusammenfassung in einem Absatz zu verfassen, präsentiere ich lieber einige Thesen:

- Spam ist ein nicht einfach zu definierender Begriff. Mit der Definition variieren auch Lösungen und politische Zielsetzungen.
- Datenschutz und die Herkunft der Adressen spielen eine wichtige Rolle. Ein weltweites Recht auf Datenschutz ist eine Lösung.
- Ein unkoordiniertes Nebeneinander von opt-in und opt-out Modell ist zumindest für die eine Hälfte keine Lösung.
- Die parallele Existenz von opt-in und opt-out Modellen ist möglich. Eine Koordination hierfür ist nötig. EU und USA müssen zusammenarbeiten. Internationale Kooperation ist notwendig. (Wäre eine Begleitung durch - zivilgesellschaftliche - Nicht-Regierungsorganisationen nicht notwendig?)
- Im Verlauf des Jahres 2004 hat es keine Weiterentwicklung regulatorischer Maßnahmen gegeben. Diese steht 2005/06 an.
- Die Spam-Bekämpfung kann von anderen IT-Problemstellungen beeinflusst werden, wie sie diese auch beeinflusse kann.
- **Das Scheitern von regulatorischen Maßnahmen über Marktmechanismen, durch gesetzliche Sanktionen und die Veränderung von Normen bestärkt Veränderungen am Code des Internets, die eine möglichst starke Form der Authentifizierung der Absender erforderlich machen.** Zuweit verbreitete und starke Formen der Authentifizierung beschränken Anonymität, Pseudonymität und verhindern *privacy*.

Der Autor, Dirk A. Schmidt, kann unter Dirk.Schmidt@netzbuch.de oder Dirk.A.Schmidt@zmi.uni-giessen.de erreicht werden.
(Dirk Schmidt, Postfach 10 23 51, D-44723 Bochum)