*Justus-Liebig-Universität Gießen*

Fachbereich Sozial- und Kulturwissenschaften
Institut für Politikwissenschaften

*Magisterarbeit*

# 'Spam' in neuen Informations- und Kommunikationstechnologien

## *Wirkung und politisch-rechtliche Bekämpfung unerwünschter Information*

Betreuer

*Prof. Dr. Claus Leggewie*

Verfasser

*Dirk Schmidt*

Girondelle 88, D-44799 Bochum

Bochum, 24. Februar 2004

# Inhaltsverzeichnis

## Einleitung

> »Doch die groß angelegte Bandbreitenverschmutzung durch Massenrundsendungen ist schließlich nichts anderes als das in den Schwachsinn verkehrte Versprechen, dass jeder Mensch von nun an potenziell mit allen anderen kommunizieren könne.« [Schneider 2001] (S.110)

Email ist ein extrem wichtiges und populäres Kommunikationsmittel, das immer mehr Nutzer in seinen Bann zieht. Es ist billig, weltweit verfügbar und simpel in der Bedienung. Der Traum, mit jedem ganz einfach und unproblematisch in Kontakt zu treten, hat jedoch eine Schattenseite: Jeder kann ganz einfach und unproblematisch mit einem in Kontakt treten. Dies wird dann zum Ärgernis, wenn die Zahl der Emails Mengen erreicht, die für den einzelnen nicht mehr verarbeitbar sind. Wenn die Verarbeitungskapzität des Einzelnen nicht mehr ausreicht, dann wird von information overload oder data smog [Schenk 1997] gesprochen:

> »E-Mail overload occurs when the number of e-mails being sent and received becomes too difficult to mange, overwhelming the user.« [Ingham 2003]

Auch wenn [Ingham 2003] spam als ein Problem des Email-Dienstes identifiziert, so handelt diese Arbeit nicht vom information overload. Dies würde bedeuten, dass Probleme mit der Aufnahme und Verwaltung von Informationen bestehen. Es ist weniger. Das Aussortieren und Löschen unerwünschter Information stellt sich inzwischen als ein großes Problem dar. Nicht die Flut an Information, sondern die Flut an unerwünschter Information – ja, sinnlosen Datenmülls - ist ein Problem. Offenbar werden Einschränkungen benötigt, wann jemand mit jemandem kommunizieren darf.

Inseln gleichen die erwünschten Informationen in gefluteten Email-Postfächern, blogs, Suchmaschinen und usenet-Foren. Spam hat für alle Nutzer keinerlei Informationswert. Keinerlei Informationwert? Leider für einige wenige schon, die dafür sorgen, dass sich spam immer noch lohnt. Diesen wenigen verdanken alle die Flut.

> »Spam wird es wahrscheinlich so lange geben, wie es Menschen gibt, die darauf hereinfallen.« (ebenda)

Auch wenn bisher noch keine Lösung für das spam-Problem gefunden wurde, so will diese Arbeit zeigen, dass es Lösungen gibt, dass an ihnen gearbeitet wird und dass unterschiedliche Lösungen vereinbar sind. Sie warnt aber auch vor den Folgen einiger Lösungen, insbesondere vor Lösungen, die eine verstärkte Kontrolle der Nutzer befördern.

Der erste Abschnitt dieser Arbeit stellt die spam-Phänome des Internets dar. Dies erfolgt ausführlich, um zum einen an den Kern dessen heranzugelangen, was spam semantisch meint, da für 'spam' bisher keine einheitliche Definition existiert, ja nicht einmal das Medium oder der Dienst genau feststeht. Zum anderen zeigt sich, welche Lösungen - allen voran beim usenet - gegangen worden sind bzw. werden können und inweit die Technik des Internets durch sie politische und gesellschaftliche Entscheidungen im Sinne der Techniksoziologie determiniert.

Dass der Email-Dienst derzeit das eigentliche Problem darstellt, wird dann anhand seines Ausmaßes seines spam-Problems geklärt. Dies führt aber nicht zu einer Definition. Vielmehr müssen unterschiedliche Definitionen unterschieden werden. Die entwickelten Kriterien einer inhaltlichen und einer formellen Definition werden dann als Instrument zur weiteren Untersuchung genutzt. Zunächst wird jedoch die gängige Typologie von Schwartz und Garfinkel dargelegt und aufgrund des verheerenden Zusammengehens von Viren und spam in 2003 erweitert, bevor die Bekämpfung von spam erläutert wird. Das Instrument der beiden Definition wird hier zum ersten Mal produktiv und klärt die unterschiedlichen Arten, spam automatisiert zu filtern, also aus dem Internet zu löschen. Der Abschnitt klärt weiterhin den Einfluss von spam auf den Email-Dienst insgesamt und legt die Ökonomie des spam dar.

Der zweite – weitaus interessantere - Abschnitt widmet sich der eigentlich politisch-rechtlichen Problemstellung von spam, nachdem der erste Abschnitt geklärt hat, welche Sorte spam überhaupt auf der Agenda der politischen Akteure steht. Die unterschiedliche Behandlung von spam, die aus einer unterschiedlichen Definition von spam und unterschiedlichen Präferenzen der definerenden Akteure herrührt, wird hier dargelegt. Das besondere Interesse gilt stellvertretend den USA und der EU, die zunächst scheinbar gegensätzliche Modelle entwickelt haben. Engagiert zeigt diese Arbeit, dass beide dennoch vereinbar sind und dass eine Kooperation in der spam-Bekämpfung lohnend ist, wie sie auch bereits anfänglich zu erkennen ist.

Der dritte Abschnitt - „Nebeneffekte“ widmet sich Konsequenzen, die aus dem Scheitern einer Kooperation drohen. An erster Stelle ist hier ein höheres Maß an Kontrolle einhergehend mit einer geringeren Möglichkeit zur Anonymität zu nennen.

Es folgt eine Zusammenfassung der Thesen dieser Arbeit und ein Fazit.

Die meisten Daten hinsichtlich spam existieren für die USA. Sofern nicht anders angegeben, wird davon ausgegangen, dass sie für die gesamte Netzwelt gelten und auf die EU bzw. Europa übertragen werden können.

# 1. Spam in neuen IuK-Technologien

Zunächst wird die Herkunft des Wortes spam geklärt und was es semantisch über die als 'spam' bezeichneten Phänomene aussagt. Anschließend werden die unterschiedlichen spam-Phänome des Internets behandelt. Durch diese Einschränkung werden SMS spam , der im Medium der Mobiltelefone auftaucht (vgl. [Dotinga 2003]), und unerwünscht zugesandte Faxe von der Behandlung ausgeklammert. Beides sind hinsichtlich der Entwicklung in Europa ältere Erscheinungen, die von den gesetzlichen Regelung, die in dieser Arbeit behandelt werden, ebenfalls abgedeckt werden, jedoch jeweils auf einer wesentlich anderen Technologie beruhen und einer anderen Ökonomie als spam im Internet folgen, da die Kosten pro Fax bzw. SMS wesentlich höher sind.

## *SPAM und spam*

Waitress: Well, there's spam, egg, sausage and spam.
That's not got much spam in it.

Mrs. Bun: I don't want any spam!

*Aus Monthy Python's Flying Circus: The SPAM Sketch*

In einem zumindest in Großbritannien berühmten Sketch der Comedy-Gruppe Monthy Python versucht ein Kunde in einem Restaurant ein Frühstück ohne das Dosenfleisch der Marke SPAM zu bestellen. Dies gestaltet sich als schwierig, da sämtliche Gerichte auf der Speisekarte SPAM enthalten. Dosenfleisch der Marke SPAM, ein Produkt der us-amerikanischen Firma Hormel Food Inc., war im Gegensatz zu den meisten übrigen fleischlichen Lebensmitteln in Großbritannien während des zweiten Weltkrieges und der ersten Nachkriegsjahre nicht rationiert. Es war überall und vielfach auch als einziges zu bekommen und die Briten wurden es Leid, wie Mrs. Bun im Sketch, in dem ein Wikinger-Chor im Hintergrund das Wort SPAM in einem fort wiederholt. SPAM gibt es in dem Sketch zu Hauf, immer und in jeglicher Kombination. Das „Entnervt-Sein“ von Mrs. Bun und ihr Wunsch, überhaupt kein SPAM bekommen zu wollen, kennen auch zahlreiche Nutzer des Internets und so kamen die spam-Phänomene zu ihrem Namen. (vgl. u.a. [Glasner 2001])

Eine weitere Analogie der spam-Phänome zum SPAM-Sketch besteht in der SPAM-Flut bzw. spam-Flut, die Monthy Python durch das endlos wirkende Repetieren des Wortes SPAM durch einen Wikinger-Chor und die Bedienung darstellt. Die Analogien zum Sketch und die darauf beruhende Benennung der spam-Phänomene führt zu einer ersten Arbeitsdefinition, was spam ist.

Spam bezeichnet das Phänomen einer großen Menge, einer Flut, an unerwünschten Informationen. Zugleich bezeichnet spam auch die einzelne unerwünschte Information, die Teil des spam-Phänomens ist. Zur Klarstellung des Unterschieds wird letztes gelegentlich auch als spam mail bezeichnet.

> „Im Internet wurde das Wort zuerst in chat-Rooms und in Adventure-Spielen für mehrere Benutzer (MUDs, multiuser Dungeons) verwendet. Nach Aussagen von Jennifer Smith, der Autorin der Frequently Asked Questions-Liste (FAQ, häufig gestellte Fragen) der Newsgruppenhierarchie *rec.games.mud* fingen einige Missetäter in Chat-Rooms damit an, dieselbe Nachricht immer wieder zu «sagen» und den gesamten Bildschirm auszufüllen, und andere Leute nannten diese Nachrichten «Spam». Es handelte sich wie im Monty Python-Sketch um sinnlose Wiederholungen.
>
> Von der Bildschirmüberschwemmung mit Wortwiederholungen zur Mailbox- oder Newsgruppen-Überschwemmung mit wiederholten Nachrichten ist es kein weiter Weg.“ [Schwartz 1999] (S.17)

## Suchmaschinen-spam

„Neue Spam-Mafia – So wird Google mit Cyber-Müll lahm gelegt“ titelt die Computerzeitschrift tomorrow auf ihrer Oktober-Ausgabe 2003 [Becker 2003]. Dort wird der „Such-Experte“ Alan Webb mit seiner Definition zu Suchmaschinen-spam zitiert: „Spam ist es dann, wenn eine Webseite nicht das bietet, was der Suchmaschinen-Eintrag verspricht.“ Der Artikel schildert, wie Suchmaschinen – allen voran die bedeutende Suchmaschine Google – mit Informationen – spam – gefüttert werden, die Webseiten bessere Positionen bei Suchanfragen besorgen. Der Autor führt aus:

> „Die Schuld an miesen Ergebnissen trifft nicht die Suchanbieter. Verantwortlich ist vielmehr eine kleine Gruppe von Webmastern die Suchmaschinen-Spammer. Sie manipulieren ihre Webseiten – und zwar Zehn- bis Hunderttausende – so, dass jede Suchmaschine sie als höchst relevant einstuft, unabhängig von der wahren Qualität des Inhalts.“(ebenda)

Die Dialektik von „wenigen“ und „vielen“ tritt hier hervor: Eine kleine Gruppe verursacht ein Problem für viele Nutzer oder sogar alle. Dies geschieht zudem schuldhaft und vorsätzlich, nicht zufällig, sondern durch „manipulieren“.
Diese Sorte spam, mit der die Suchmaschinen gefüttert werden, wird zudem eigentlich als wertlos, ohne jeglichen informationellen Mehrwert für den Nutzer der Suchmaschinen und somit als „Cyber-Müll“ bezeichnet.

## Blog-spam

Wired News titelte am 26. Oktober 2002 „When the Spam Hits the Blogs“[Delio 2002a]. Blogs sind automatisierte elektronische Tagebücher, in die einer oder mehrere Nutzer regelmäßig Berichte zum Thema des blogs eintragen. Eine erste Form von spam kann hier darin bestehen, dass ähnlich dem usenet spam unpassende Beiträge in die blogs selber eingestellt werden. Der Artikel stellt jedoch auf eine bestimmte Form von blogs ab. Es existieren bei zahlreichen blogs sogenannte referral logs. Dies sind automatisch generierte Listen, die aus den Links erzeugt werden, über die die Nutzer zu einem blog gelangen. In der Regel entstehen hierdurch Linklisten, die auf inhaltlich verwandte Seiten verweisen, wobei die Seiten als relevanter dargestellt sind, je mehr Nutzer über einen Link von diesen zum blog gekommen sind. Die spam-Flut besteht nun darin, dass spammer auf den von ihnen beworbenen Seiten zahlreiche Links zu blogs mit referral logs unterbringen und darüber die blog-Seiten aufrufen lassen, um ihre inhaltlich fremden Seiten in den referal logs zu positionieren. Dies zerstört den Wert dieser referal logs, wie auch das Veröffentlichen nicht zum Thema eines blogs passender Informationen diesen seines Sinnes und schließlich seiner Nutzer beraubt. Michelle Delio führt hierzu aus:

> »But bloggers said that log spam is far more than just an annoyance: „On top of the fact that this is obnoxious and instrusive, it completely destroys the entire point of referral log.“ said August J. Pollak, cartoonist for the XQUZYPHYR and Overboard blog. „If hundreds of spammers start spamming logs, then people will eventually stop using logs.“« [Delio 2002a]

Die Gefahr besteht, dass spamming dazu führt, dass die Dienste nicht mehr genutzt werden. ([Intern 2003a] beschreibt eine weitere Form dieses spams bei blogs, den comment spam, der über die Kommentare zu blog-Beiträgen eingefügt wird.)

## Messenger Service spam

Bei Messenger Service spam handelt es sich um spam, der über den Microsoft Windows Messenger Service verschickt wird. Der Microsoft Messenger Service ist nicht mit dem gleichnamigen Programm Microsoft Messenger zu verwechseln. Der Messenger Service ist eine Funktion der Microsoft Windows Betriebssysteme, der es Administratoren von Intranets ermöglichen soll, auf die Oberfläche der Nutzer eine kurze Nachricht zu schicken. Bei den Windows-Versionen 2000, NT und XP ist dieser Service standardmäßig aktiviert, so dass ohne Nutzereingriff entsprechend spam empfangen wird. Für künftige Auslieferungen hat Microsoft zugesagt, den

Messenger Service standardmäßig zu deaktivieren. (vgl. [McWilliams 2003])[1]

Dieser Messenger Service kann benutzt werden, um zehntausende an Nachrichten, die wie Systemmeldungen aussehen, auf die Bildschirme von Anwendern zu senden. Spammer nennen diese Form auch IP-Marketing. Das Abschalten des Messinger Service oder der Einsatz einer firewall, die nur erwünschte Zugriffe auf die Rechner eines Internets gestattet, genügt schon, um das Ärgernis dieses spam-Phänomens zu beseitigen.

Die FTC hat eine Firma verklagt, die per Messenger spam für ihr eines ihrer Produkte warb, das Schutz vor dieser Art von spam bot:

> »The FTC, however, compared D-Squared to vandals throwing bricks through windows to sell home-security systems. It said the company's founders "desperately try to recast themselves as innocent public servants who merely hope to warn consumers about a security flaw."« [AP 2003b]

Hier findet sich das Motiv, das per spam antispam-Software beworben wird. Die Inhalte dieser Form von spam sind ansonsten die gleichen wie bei email spam. (neben den genannten Berichten von Wired News, siehe auch die weitere Berichterstattung: [AP 2003a], [AP 2003c], [Reuters 2003c])

## usenet spam

Alan Schwartz und Simson Garfinkel sehen den Beginn des spam-Phänomens im usenet in der Mitte der 1990er Jahre:

> »Zuerst erkannte die amerikanische Rechtsanwaltskanzlei Canter & Sigel 1994 den Wert des Usenet für die Anreicherung des eigenen Kundestammes. Das sogenannte 'Greencard-Posting' hat seither viele Nachahmer gefunden. Was als Ärgernis begann, wurde bald zur permanenten Störung des Netzfriedens. Überflüssige Werbung und ärgerliche Kettenbriefe werden seither hemmungslos in allen Gruppen des Usenet verbreitet.« [Bohne 2002]

Kommerzielle Interessen, günstige Werbung für eine Dienstleistung, stand Pate bei der Geburt von spam im usenet. Wie bei blog-spam besteht die Gefahr, dass die betroffenen Newsgruppen für Nutzer aufgrund der Flut an unerwünschter Information keinen Wert mehr haben, diese nicht mehr genutzt werden und so das Medium usenet zerstört wird.

Schwartz und Garfinkel unterscheiden in ihrem Buch sechs Unterformen von spam [Schwartz 1999] (S.19f). Spam im engeren Sinn sei dabei das exzessive Mehrfachver-

1 AOL deaktiviert über seine Zugangssoftware den Messenger Service. Dies ist keine Funktion des Programms, sondern des Betriebssystems. Fraglich ist, inwieweit dies einen unzulässigen Zugriff auf den Rechner des Nutzers darstellt. - vgl. [Intern 2003b]

senden (excessive multi-posting, EMP) eines Artikels in einer Gruppe, das Fluten mit immer dem gleichen Inhalt. Das exzessive Querversenden (ECP, excessive cross-posting) beschreibt das Versenden eines Artikel an mehrere Newsgruppen. Das Mehrfachversenden eines Artikels an passende Newsgruppen ist zwar erwünscht, allerdings stellt das gleichzeitige Versenden an Hunderte von Newsgruppen einen Mißbrauch des usenet, einen Verstoß gegen die Netiquette dar. Ein sogenannter spew unterscheidet sich von einer exzessiven Mehrfachversendung durch seine Ursache, die in einem falsch konfigurierten Programm des Nutzers besteht und zu einem mehrmaligen Versenden des gleichen Artikels führt. Off-topic posting sind in Schwartz' und Garfinkels Einteilung Artikel, die in einer thematisch nicht passenden Newsgruppe stehen. Die meisten Newsgruppen verfügen über eine Charter, die definiert, welche Themen gewünscht und welche unerwünscht sind. Die letzten beiden Gruppen, binaries und commercial postings, stellen entsprechende Verstöße gegen diese Charter da. Für jede Newsgruppe ist festgelegt, ob binaries – kodierte Binärdateien, wie zum Beispiel Bilder oder Programme – oder Werbung erwünscht sind. Ende der 1990er Jahre etablierte sich das System der usenet death penalty, das Beiträge von Nutzern oder Servern, die gegen die jeweilige Charter verstoßen (spam, Pornographie) weltweit effektiv löscht, ohne dass sie von einem Nutzer zunächst heruntergeladen werden müssen:

> „It gives ISPs a very strong incentive to be vigilant themselves not to harbour spam or offensive content.“ [EU-Studie 2001] (S.19)

## email spam

Im Bereich des auf den Protokollen POP3[2] und SMTP basierenden Email-Dienstes[3] existiert aufgrund seines noch darzulegenden Ausmaßes das eigentliche spam-Problem. Dies liegt zum einen am großen Anteil von spam mails an allen Emails, zum anderen an der großen Bedeutung des Email-Dienstes für das Internet. Email ist die Killer Applikation ("killer app") des Internets. Als Beispiel sei angeführt, dass 82% der schweizer Internetnutzer Email nutzen.[4] Große Bedeutung kommt Email im privaten als auch im geschäftlichen Bereich zu: Es dient als Arbeitsmittel und der Pflege sozialer Kontakte. Zahlen für den Umfang des Email-Verkehrs sind schwer zu benennen. Fallows schätzt den Umfang auf täglich 30 Milliarden Emails, wovon etwa die Hälfte auf spam entfällt. Fallows ermittelt einen Unterschied des Umfangs an

2 POP3: post office protocoll (version) 3 – Prokoll für den Empfang von Email
3 SMTP: simple mail transfer protcoll – Protokoll für den Versand von Emails
4 Zahlen für 2002 aus einem Vortrag des Schweizer Datenschutzforums [Heinzmann 2002], an zweiter Stelle liegt die Nutzung von Suchmaschinen mit 60%. In den USA ist Email die beliebteste Nutzungsform des Internets. 93% der erwachsenen, amerikanischen Netznutzer nutzen den Email-Dienst, dies entspricht 117 Millionen Nutzern. - Zahlen siehe [Fallows 2003], S.6

spam im privaten und im geschäftlichen Emailverkehr. Privatpersonen erhalten demnach weniger Emails, aber der spam-Anteil ist geringer. Allerdings ist der Zeitverbrauch für den geschäftlich erhaltenen spam etwas höher (ebd., S.16f). Nach Angaben von Ferris Research [Ferris 2003a] liegt der Anteil an spam 2002 bei 15-20% in den Intranets von Firmen, bei 30% in den Netzen der internet service provider (ISPs); für 2003 und 2004 berichten andere Quellen von bis zu 60% spam-Anteil.
(vgl u.a. [Glasner 2004], [Singel 2003])

Die Kosten die amerikanischen Firmen durch spam entstehen werden auf 10 Milliarden Dollar in 2003 geschätzt - pro Tag und Arbeitsplatz sind dies $ 14 (ebenda). Hierbei darf nicht vergessen werden, dass der Nutzer nur einen Teil des spams sieht, nur den Teil, der in seinem Posteingangsordner ankommt. Den Teil, den der Server (bzw. ISP) nicht zustellen kann oder bereits herausfiltert, bekommt der Nutzer gar nicht erst zu sehen. Das Aufkommen an erfolgreich zugestellter spam ist geringer als der Anteil an spam insgesamt und wiederum geringer als das durch spam verursachte Überrtragungsvolumen, da auch noch der error traffic, Meldungen über nicht erfolgreich zugestellte Emails, mit einzurechnen ist. Bei nicht-existenten Absenderadressen in spam mails , kann der error traffic wiederum error traffic erzeugen.

Abgesehen von den großen Übertragungsvolumina und damit den Kosten an Zeit und Geld ist auch zu beachten, dass durch spam die Akzeptanz des Email-Dienstes bei Nutzern und potentiellen Neu-Nutzern reduziert wird. Nach [Fallows 2003] sagen 70% der Nutzer, dass spam die Nutzung des Internets subjektiv beeinträchtigt ("unpleasant and annoyed"), 27% der Email-Nutzer sähen spam als großes Problem an, 59% eher als ein kleines Problem und 14% als überhaupt kein Problem (ebd., S.27).

Tabelle 1 und Abbildung 1 geben eine Darstellung der Zahlen von [Fallows 2003], die belegen, dass es mehr berufliche Emails als private gibt.

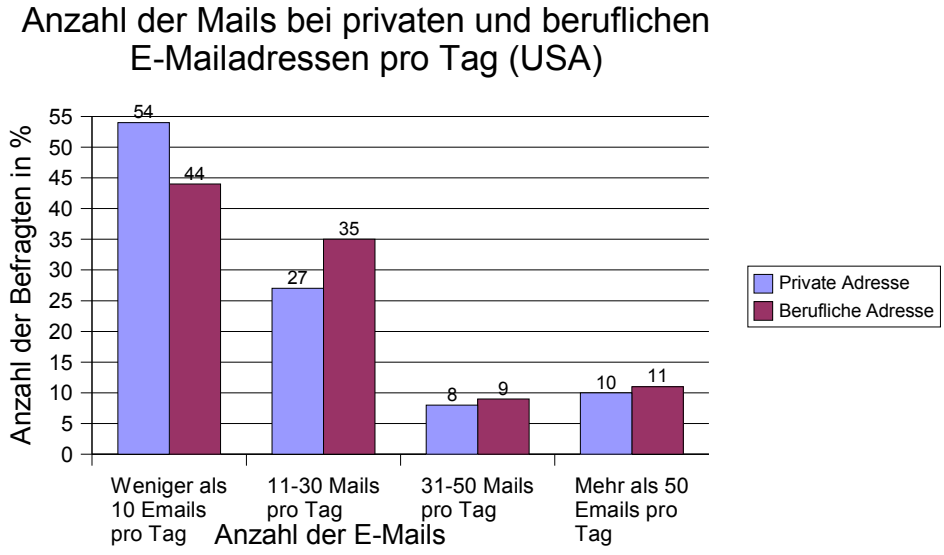


*Abbildung 1 Anzahl der Emails bei privaten und beruflichen Email-Adressen*

| Email | Private Adresse | Berufliche Adresse |
|---|---|---|
| Weniger als 10 Emails pro Tag | 54 % | 44 % |
| 11-30 Mails pro Tag | 27 % | 35 % |
| 31-50 Mails pro Tag | 8 % | 9 % |
| Mehr als 50 Emails pro Tag | 10 % | 11 % |

*Tabelle 1 Anzahl der Emails bei privaten und beruflichen Email-Adressen*

Dem gegenüber steht der Befund von Tabelle 2 und Abbildung 2, dass der Anteil an spam unter den beruflich empfangenen Emails geringer ist. Dies führt die Studie auf drei Gründe zurück ( S.19):

1. Private Email-Adressen seien verletzlicher als beruflich genutzte, da die großen Anbieter von Email-Dienstleistungen für Private lohnenswerte Ziel für Angriffe von Spammern seinen und
2. da die Nutzer mit ihren privaten Email-Adressen ungezwungener („cavalierly“) umgingen, während bei beruflichen Adressen größere Vorsicht herrsche.
3. In Firmen seien die Abwehrmaßnahmen gegen spam größer, mehr antispam-Software werde verwendet.

Zwar seien der Studie nach Zeit und Geld Verbrauch durch spam am Arbeitsplatz geringer, allerdings liege das daran, dass dem durchschnittlichen Arbeitnehmer die Kosten für die Abwehrmaßnahmen verborgen blieben.

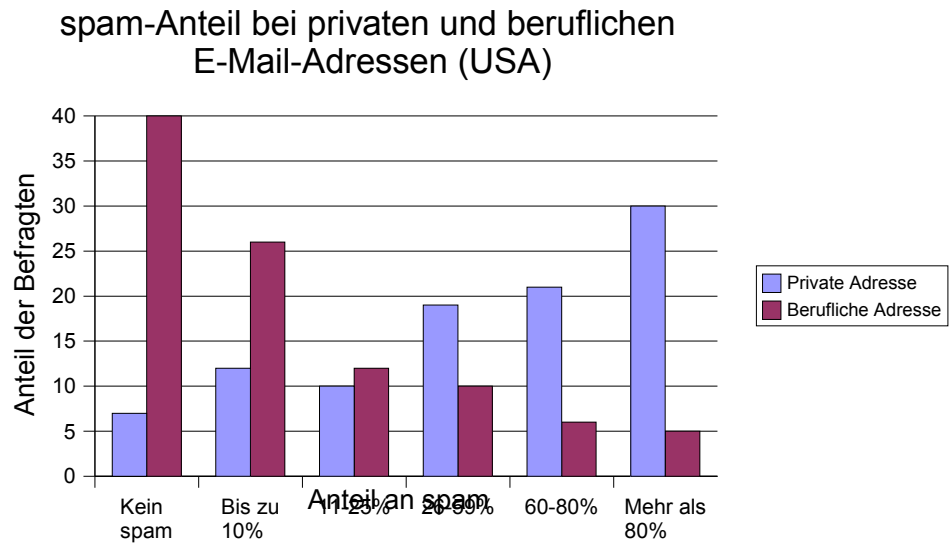


*Abbildung 2 spam-Anteil bei beruflichen und privaten Email-Adressen*

| Email | Private Adresse | Berufliche Adresse |
|---|---|---|
| Kein spam | 7 | 40 |
| Bis zu 10% | 12 | 26 |
| 11-25% | 10 | 12 |
| 26-59% | 19 | 10 |
| 60-80% | 21 | 6 |
| Mehr als 80% | 30 | 5 |

*Tabelle 2 spam-Anteil bei beruflichen und privaten Email-Adressen*

Inwieweit sich spam als Problem für den einzelnen Nutzer darstellt, ist nach Alter und Geschlecht zu differenzieren. Frauen (83%) sind beunruhigter über spam als Männer (68%), junge Menschen (17-29) sind toleranter (32%) als ältere (18%).

Die Gefahr im hohen spam Aufkommen besteht darin, dass die Akzeptanz von Email verringert wird. Emails betrügerischen und zweifelhaften Inhalts sind hierfür besonders verantwortlich, wie auch die eingesetzte Filtertechnologie, die befürchten lässt, dass eigene Emails nicht den Empfänger erreichen (false positives). Diese Befürchtungen werden weiter verstärkt, da der Kampf zwischen Spammern und anti-Spammern einem Katz-und-Maus-Spiel gleicht, das den durchschnittlichen Nutzer selber vor eine Sisyphos-Aufgabe stellt.

Weiterhin ist gar nicht genau definiert ist, was spam eigentlich ist. Es existiert eine

verwirrende Anzahl an teilweise gegensätzlichen Definitionen. Die Grenzen zwischen verschiedenen Formen des spam – auch des email spam – sind fließend. Eine Definition, ob eine Email spam ist, scheint dabei vom Inhalt und vom Absender abhängig zu sein. Der kleinste gemeinsame Nenner ist, dass spam auf eine unerwünscht zugesandte Email (unsolicited bulk email – UCE) ist, deren Absender der Empfänger nicht kennt und deren Inhalt kommerzieller Natur ist. Nach [Fallows 2003] bezeichnen 92% der amerikanischen Internetnutzer eine derartige Email als spam. Alle übrigen Definitionen, die weitere Emails erfassen, erreichen prozentual weniger Zustimmung.

| **What Emailers Consider Spam**<br>Emailers' definition of spam depends on the sender and the subject matter of the message | |
|---|---|
| **Sender or Subject Matter** | **% Who consider it Spam** |
| Unsolicited commercial email (UCE) from a sender you don't know | 92 |
| UCE from a political or advocacy gorup | 74 |
| UCE from a non-profit or charity | 65 |
| UCE from a sender with whom you've done business | 32 |
| UCE from a sener you have given permission to connect you | 11 |
| UCE containing Adult content | 92 |
| UCE with investments deals, financial offers, moneymaking proposals | 89 |
| UCE with product or service offers | 81 |
| UCE with software offers | 78 |
| UCE with health, beauty, or medical offers | 78 |
| Unsolicited email with political mesages | 76 |
| Unsolicited email with religious information | 76 |
| A personal or professional message from one you don't know | 74 |
| Quelle: Pew Internt & American Life Project June 2003 Survey. For items 1-5, N=624. Margin of error is +/-4.2%. For items 6-13, N=648. Margin of error is +/-4.1% [Fallows 2003] | |

*Tabelle 3 Die Definition der Nutzer zu spam*

## *Was ist spam?*

Die grundlegenden Elemente von spam sind vier: der Absender (from), der Betreff (subject), die routing information – die Information welchen Weg die Email über welche Server genommen hat – und der eigentliche Nachrichtenkörper („body“), die eigentliche Nachricht. Sind diese vier Elemente noch einfach zu identifizieren, so schwierig und unscharf sind Fragen zu beantworten, die sich zu den Elementen

stellen:

- Sind die Absender, die, die sie vorgeben zu sein? Kann man sie kontaktierten? Funktioniert die Kontaktmethode?
- Ist der Betreff irreführend oder offensiv? Gibt sich die Email schon im Betreff als Werbung bzw. spam zu erkennen?
- Ist der Inhalt, das Anliegen des Nachrichtenkörpers, legal, betrügerisch oder etwa pornographischen Inhalts?
- Sollte jegliche Form an unerwünschter Werbung – spam - gleich behandelt werden oder gibt es bevorzugte Formen an spam? Gibt es spam mit besonderem Inhalt, zum Beispiel politischem oder religiösen Inhalt?
- Hatte der Absender das Recht, den Empfänger zu kontaktieren? Hatte der Absender eine Erlaubnis hierzu?

Einige Elemente und Fragen richten sich mehr auf formelle Aspekte einer Email, anderen auf inhaltliche Kriterien. Die Definition von spam und damit ihre Identifikation wird dadurch erschwert, dass die inhaltliche Bedeutung der vier grundlegenden Elemente auseinanderfallen können, wenn sie nicht sogar in täuschender Absicht ohne Bezug zueinander gewählt wurden.

Spam kann nicht nur einfach anhand von Absender und Betreff indentifziert werden. Der FTC nach sind bei zwei Drittel von spam falsche oder irreführende Informationen in Absender oder Betreff vorhanden, die mit dem Inhalt nichts zu tun haben, ja geschwindelt oder betrügerisch („bogus“) sind (siehe [FTC 2003], [Wired News 2003a]).

Im Betreff werden oft Texte verwendet, die im Sinne von social engineering erstellt wurden, um den Empfänger zum Öffnen und somit Lesen der Emails bewegen sollen. Falsche Absenderangaben, die vorgeben ein Bekannter oder sogar man selber sei Urheber der Email, nutzen ebenfalls ein Kalkül im Sinne von social engineering, was darauf hinweist, dass spam nicht nur eine technische Dimension hat[5]. Teilweise werden aber auch die Email-Adressen gekidnappt („hijacked“) und zumindest im technischen Sinne spam  mit realen Absendern versehen, die dann fälschlicherweise als Urheber dieser Emails angesehen werden.(vgl u.a. [Bruns 2003]) Dies hat negative Konsequenzen auch für die, deren Adressen gekidnappt wurden, da diese mit

5 Auf die große Bedeutung von scoial engineering beim Mißbrauch von IT-Ressourcen weist das vom weltweit bekannten Hacker Kevin Mitnick in Zusammenarbeit mit William Simon verfasste Buch zum Thema Hacke mit dem deutschen Titel „Risikofaktor Mensch. Die Kunst der Täuschung“ hin. [Mitnick 20003]

Beschwerden und error traffic zu kämpfen haben, ja ihre eigenen – regulären - Emails als spam aussortiert werden (false positives).

Damit spam unterschiedliche Abwehrmaßnahmen umgehen kann und überhaupt vom Nutzer geöffnet wird, werden häufig neben Absenderangaben auch die routing information über den Weg, den die Email durchs Internet nahm, gefälscht. Der Nachrichtenkörper wird von Bulk Email-Programmen automatisch verändert oder mit Spamfutter, für den Nutzer sinnlose Daten, ergänzt, damit diese Metamorphose des für Menschen immer noch gleichen Inhalts, spam für Filter möglichst unkenntlich macht. Vielfach ist der Nachrichtenkörper von seinem Anliegen her betrügerisch, zum Beispiel bei Kettenbriefen (MMF).

Zur weiteren Untersuchung der Möglichkeiten einer Bekämpfung von spam sei zwischen einer formellen und einer inhaltlichen Definition von spam unterschieden.

## Die formelle Definition von spam

Die formelle Definition von spam verwendet formale Kriterien, wie zum Beispiel die Absenderangabe, und auch Metadaten zu einer Email, die zum Beispiel durch das Wissen um den Mehrfachversand bei Servern und Providern anfallen.

> »Definition of spam
>
> A "spam" e-mail is generally defined as an unsolicited mailing, usually to many people. A message written for, and mailed to, one individual that is known to the sender is not spam, and a reply to an e-mail is not spam, unless the "reply" repeats endlessly.« [Lutus 2003]

Spam ist im weitesten Sinne eine unangefordert zugesandte Email (unsolicited mail). Diese Definition greift aber viel zu weit, da sie jede Email umfasst, die auch am Anfang einer Kommunikation steht, die nicht von einem selber ausgegangen ist. Wenn alle unfreiwillig zugesandten Emails gelöscht würden, dann könnten viele Kommunikationen per Email nicht zustande kommen. Fraglich ist auch, ob spam nicht auch aus Emails bestehen kann, zu deren Zusendung durch einen bestimmten Absender einmal eine Einwilligung erteilt wurde, der Inhalt der Emails sich aber derartig verändert hat, dass er nun auch spam darstellt (Problem der false positives).

Als weiteres Kriterium unfreiwilliger Zusendung wird daher meist noch der massenhafte Versand inhaltsgleicher Emails genommen (unsolicited mass email). Dabei spielt eine Personalisierung der einzelnen Emails keine Rolle, bei der wie bei einem Serienbrief nicht nur die Anschrift – die Email-Adresse -, sondern auch die Anrede ausgetauscht wird. Problematisch bei der Erkennung von spam ist hier, dass das Krite-

rium „massenhaft“ vom einzelnen Empfänger kaum erkannt werden kann, da er in der Regel nur über Informationen über die eine Email verfügt, die er bekommen hat. Regelmäßig enthält spam gerade nicht die Information, an wen sie noch gegangen ist, sondern will gerade vortäuschen, nur für einen Empfänger – mich – bestimmt zu sein (social engineering). Daher tritt zu dieser Definition häufig noch als Abgrenzungskriterium eine Definition hinzu, was nicht spam ist.

Eine Email, die nur für einen Emfpänger bestimmt ist und nur für ihn verfasst wurde, ist kein spam. Aber auch dies lässt sich nicht feststellen, wenn nicht Informationen über alle insgesamt versandten Emails vorliegen. Erst dass zusätzliche Kriterium, dass der Sender dem Empfänger bekannt zu sein hat, macht es möglich, Post als spam zu identifizieren. Wirklich? Was ist mit Post, die an jemanden gerichtet ist, der den Absender noch nicht kennt? Was ist mit bestellten Massenmailings?

Zwischen der Definition, was spam ist, und der Definition, was nicht spam ist, gibt es eine große Lücke der Uneindeutigkeit. Ist es auf der einen Seite nicht möglich, eine Email eindeutig als Massenaussendung zu identifizieren, ist es auf der anderen Seite kaum möglich anhand weniger Kriterien festzustellen, ob eine Email von einem bekannten Absender herrührt oder im Anschluss an frühere Kommunikationen – auch außerhalb des Internets – erfolgt.

Als weiteres Kriterium für spam können auch einige Annahmen über die Absenderadressen herangezogen werden, da aufgrund der Entwicklung des Umgangs mit spam inzwischen vielfach nicht existierende – fiktive – Absenderadressen benutzt werden.

## Die inhaltliche Definition von spam

Wie James Gleick in seinem Artikel „You have spam“[6] [Gleick 2003] schildert, hat spam inhaltlich nur wenige Themen mit einigen Variationen zu bieten. Da der Großteil an spam in den Mailboxen englischsprachig ist – in anderssprachigen Kulturkreisen also ein weiteres Kriterium – hier die Original-Liste von James Gleick:

> »phone cards, cable descramblers, holiday prizes. Easy credit, easy weight loss, free holidays, free girlz. Inkjet cartridges and black-market Viagra, get-rich schemes and every possible form of pornography.«

Schönheitsoperationen, weitere Medikamente und Konzepte für Heimarbeit sind noch als Inhalte von spam zu ergänzen. Ein paradoxes inhaltliches Kriterium von spam ist dabei die Beteuerung, dass es sich bei einer Email gerade nicht um spam handle, was

6 (2) Der Artikel wird auf verschiedenen Seiten im Internet vollständig wiedergegeben, zum Beispiel auf http://www.australianit.news.com.au – dort zum Beispiel auch gefunden am 2. Juli 2003, veröffentlicht wurde er dort am 17. März 2003 Die Erstpublikation erfolgte am 9. Februar 2003 im New York Times Magazine. (abgedruckt aber auch in

viele spam mails behaupten.

Die FTC identifiziert die zwölf häufigsten Inhalte in spam:

| Typ des Angebots | Beschreibung | Anteil in % |
|---|---|---|
| Investment/Business Opportunity | work-at-home, franchise, chain letters, etc. | 20 |
| Adult | pornography, dating services, etc. | 18 |
| Finance | credit cards, refinancing, insurance, foreign money offers, et.c | 17 |
| Products/Services | products and services, other than those coded with greater specifivity | 16 |
| Health | dietary supplements, disease prevention, organ enlargement, etc. | 10 |
| Computers/Internet | web hosting, domain name registration, email marketing, etc. | 7 |
| Leisure/Travel | vacation properties, etc. | 2 |
| Education | diplomas, job training, etc. | 1 |
| Other | catch-all for types of offers not captured by specific categories listed above | 9 |
| Quelle: [FTC 2003], S.2. | | |

*Tabelle 4 Ein Dutzend Themen für spam*

Kriterien für die inhaltliche Filterung von Emails sind aber schwer zu entwickeln. Zwar können bestimmte Inhalte herausgefiltert werden, aber es werden auch Kriterien benötigt, wann es sich bei einer Email nicht um spam handelt. Alleine das Vorhandensein von phone cards in einer Email als Löschkriterium könnte fatale Folgen haben, insbesondere wenn ich damit handel oder einen Prozess hierzu führe. Hilfreich ist hierbei natürlich, wenn ich Telefonkarten nur in Deutschland verkaufe. Englischsprachige Emails sollten dann seltener auftreten, sind aber dennoch nicht ganz unwahrscheinlich.

Nicht jede Email will offensichtlich etwas verkaufen. Ihre Absicht erschließt sich erst dann – wie die Benachrichtigung über den Erhalt einer elektronischen Postkarte (ecard) – wenn die zugehörige Internetseite aufgesucht wird. Manchmal verstecken sich dahinter auch Programme, so bisher die gefürchteten 0190er-Rufnummern, die dann eine Telefonverbindung zu einem kostenpflichtigen Angebot herstellten.

Formale – meta-informationelle - und inhaltliche Kriterien lassen spam erkennen.

Diese Regeln sind nicht immer trennscharf, leider auch nicht leicht zu automatisieren, da die Software alle Informationen benötigen würden, über die ein menschlicher Empfänger verfügt. So kann das Erstellen umfangreicher Listen von allen Personen, die uns potentiell eine Email schicken dürfen keine Lösung sein, wie die Aufstellung von Wortlisten, die Emails identifizieren, die wir bereit sind, noch zu lesen.

Beide Definitionen haben ihre Schwächen. Problematischer wird dies noch, wenn das Prinzip herangezogen wird, dass die Regeln zur Erkennung von spam nur spam herausfiltern dürfen, aber niemals echte Emails. Also im Zweifel wäre eine Email daher nicht als spam zu bezeichnen, um dem Risiko zu entgehen, eine Mitteilung fälschlicher Weise nicht beachtet oder sogar gelöscht zu haben. Diese falsch gefilterten Emails werden als false positives bezeichnet und stellen technisch und rechtlich ein Problem dar.

Das Gesicht der Risikogesellschaft (risk society) taucht auf (vgl.u.a. [Beck 1986]). Der Einsatz von Technik – hier Email – schafft gemäß der Logik der Risikogesellschaft neue Risiken – hier die spam-Flut. Eine Bekämpfung von spam mit Technik – informationstechnischer, sozialwissenschaftlicher oder sonst welcher – schafft wieder neue Risiken. Der Theorie der Risikogellschaft nach, kann es daher kein risikoloses Identifizieren und Filtern von Emails geben. Jede Definition von spam birgt die Gefahr, doch irgendwie echte Emails zu filtern. Schauen wir doch mal diese Arbeit als Email an. Sie umfasst die Themen:

> »phone cards, cable descramblers, holiday prizes. Easy credit, easy weight loss, free holidays, free girlz. Inkjet cartridges and black-market Viagra, get-rich schemes and every possible form of pornography.«
> (wie oben: [Gleick 2003])

Weiterhin enthalten gemäß Angabe der FTC zwei Drittel aller spam falsche Angaben im Betreff, in der Absenderabgabe und übrigen Inhalt [FTC 2003] (S.14f).

Die inhaltliche und die formelle Definition von spam stellen zwei Seiten der gleichen Medaille dar. Zum einen kann anhand scheinbar handfester Kriterien geprüft werden, ob eine Email spam ist oder nicht – ggf. müsste die Software, der Code des Internets, entsprechend programmiert sein. Zum anderen sind bestimmte Inhalte einer Email zu berücksichtigen, um sie ggf. als spam zu identifizieren. Verwiesen sei hier auf die Schwierigkeiten der empirischen Inhaltsanalyse, Inhalte semantisch korrekt zu kodieren. Keine der beiden Definitionen – besser Definitionsansätze – ist befriedigend, da er bei der derzeitigen Gestalt des Internets hinreichend Unschärfe lässt. Michelle Delio fasst das Ergebnis einer Konferenz der FTC über spam mit der Überschrift

*„Spam: Much Hated, Little Defined“* zusammen [Delio 2003f].

Diese Arbeit sieht eine formelle Definition von spam als die leistungsfähigere hinsichtlich einer brauchbaren Definition an, um den Kampf gegen spam führen zu können. Auf eine Analyse der inhaltlichen Seite kann aber bisher nicht völlig verzichtet werden, da sie Ursache vieler Problemstellungen und auch einen Beitrag zur Bekämpfung darstellt. Nicht zuletzt wurden ein großer Erfolg im oszillierenden Kampf gegen spam durch die von Paul Graham erfundenen Bayes'schen Filter errungen, die die Inhalt der Emails eines Nutzers analysieren und auf Grundlage daraus gewonnener statistischer Wahrscheinlichkeiten versuchen, spam zu identifzieren und zu filtern. Diese Entscheidung für die formelle Definition kann die vorliegende Arbeit nur im Ganzen begründen, indem sie für eine Stärkung der Kriterien der formellen Definition aufzeigt, dass dieser Weg eine Lösung darstellt, und auf die Grenzen der Filterung nach inhaltliche Kriterien hinsichtlich false positives hinweist. Letzlich ist die Filertechnik allein keine befriedigende Lösung – andere sind aber nicht sofort in Sicht.

> »There are no simple answers to the spam problem. But we have to do something now, before the usefulness of e-mail is completely destroyed.«
> (Timothy Muris, Vorsitzender der FTC bei der Eröffnung einer Konferenz über spam, zitiert nach [Delio 2003f])

### *spam-Kategorien*

Schwartz und Garfinkel unterscheiden vier Sorten an email spam [Schwartz 1999] (S.18):

- Eine **unangeforderte Werbe-Email** (unsolicited commercial email, UCE) ist eine Email, „die man nicht angefordert hat und die ein bestimmtes Produkt oder eine Dienstleistung bewirbt.“ Eine anderes Wort hierfür ist Junk-Mail.
- Eine **unangeforderte Massen-Email** (unsolicted bulk email, UBE) ist eine Email, „die als Seriennachricht an Tausende (oder Millionen) von Benutzer geschickt“ wurde. Vom Inhalt der Email hängt ab, ob es sich zugleich auch um eine Werbe-Email handelt. Es gibt aber auch andere Inhalte, zum Beispiel politische, die als unangeforderte Massen-Emails versandt werden ohne kommerzielle Natur zu sein.
- **Kettenbriefe und Hoxaes**: Kettenbriefe sind Emails, die in der Regel ein Geschäftsmodell nach dem Schema „make money fast“ (MMF) versprechen, hinter denen mehrschichtige Marketingsysteme versteckt sind. Diese Emails geben vor, dass schnell Geld verdient werden könne, und fordern in der Regeln zum Werben weiterer Kunden – unter anderem auch per Email – auf. MMF sind in der Regel betrügerisch oder unlauter und daher illegal.

Eine andere Variante von Kettenbriefen sind sogenannte hoaxes (singular hoax), die ich auch zu den Kettenbriefe hinzurechne und die Kategorie von Schwartz und Garfinkel damit erweitere. Hoaxes sind Kettenbriefe die den jeweiligen Empfänger mit ihrem Inhalt veranlassen wollen, die Email an weitere Empfänger weiterzuleiten. Es handelt sich quasi um einen Virus bzw. Wurm, der nicht den Computer infizieren will zu seiner weiteren Verbreitung, sondern den Nutzer, der seinen Inhalt liest. Auf Überschneidungs- und Kategorisierungsprobleme zwischen spam und hoaxes hat bereits Armin Medosch hingewiesen.[Medosch 2001][7]

- **Rufschädigungen** (reputation attacks) sind Emails, die vorgeben, von einer bestimmten Person oder Organisation zu kommen. Der Sinn der Täuschung besteht darin, dass die Email den Empfänger über den vorgetäuschten Absender verägern soll. Rufschädigungen sind illegal.

Den vier Kategorien von Schwartz und Garfinkel füge ich noch eine weitere hinzu:

### Trojanischen spam

Trojanischen spam teile ich in drei Unterformen, denen gemeinsam ist, dass bei ihnen nicht die Vermittlung eines semantischen Inhalts, in der Regel Werbung, im Vordergrund steht, sondern die Technik der Verbreitung bzw. die Schaffung einer Infrastruktur für den Versand von spam. Die vier Unterformen sind Wurm-Mails inkl. Viren-Mails, Trojaner und eine Form, die ich in Anlehnung an [Schwartz 1999] Spamfutter[8] nenne.

### Würmer und Viren

Wurm-Mails sind Emails, die ein Wurm, eine bestimmte Form eines Computer-Virus, zwecks seiner Verbreitung und Infizierung weiterer Computersysteme verschickt. Von der unangeforderten Massen-Email unterschiedet sich eine Wurm-Mail dadurch, dass eine eventuell mitgesendete Nachricht nur der Verschleierung der wahren Absicht dieser Email dient bzw. den Empfänger dazu bewegen soll, die angehängte Datei auszuführen, womit der Rechner mit dem Wurm infiziert wird. Meist wird hier auch social engineering angewendet. (vgl. insgesamt [Wang 2003], S.73ff)

Der eigentliche Inhalt ist eine angehängte Binärdatei, die den Wurm enthält. Der Un-

7 Ein weitere Unterscheidung dieser Kategorie in Unterkategorien hoaxes, Kettenbriefe und MMF aufgrund ihrer Inhalte wäre denkbar, schweint aber wenig produktiv zu sein, da alle die gleichen Verbreitungsweise nutzen und dies die gleiche Technik zur (technischen) Bekämpfung impliziert.

8 Schwartz und Garfinkel beschreiben eigentliche sinnlose Email-Adressen, die den sogenannten harvestern angeboten werden. Spamfutter bezieht sich hier darauf, dass sinnlose Daten als spam oder als Teil einer spam geschickt werden, um die antispam-Software – insbesondere Bayes'sche Filter – in ihrer Wirkung negativ zu beeinflussen. Es bleibt das Motiv, dass Software anderer Software sinnlosen Datenmüll „zum Fraß“ vorlegt.

terschied zwischen einem Wurm und einem Virus besteht darin, dass ein Wurm sich selber verbreiten kann. In der Regel geschieht dies per Email oder Sicherheitslücken in vernetzten bzw. ans Internet angeschlossenen Computern. Würmer, die sich per Email verbreiten werden englisch als mass-mailing worms bezeichnet und erzeugen das, was ich hier Wurm-Mail nenne. Würmer geben in der Regel auch vor, dass die Wurm-Mails von Personen stammen, die der Empfänger kennt (social engineering). Dies führt dazu, dass die Empfänger geneigter sind, dem Inhalt zu vertrauen und durch Öffnen der Email bzw. dem Starten der Binärdateien, dem Wurm Zugriff auf den Rechner zu ermöglichen. Würmer erreichen dies, in dem sie den Wirtsrechnern, in der Regel die Adressbücher von Email-Programmen, nach verwertbaren Empfängeradressen durchsuchen; teilweise beziehen sie sogar ihren vermeindlichen textuellen Inhalt und ihren Betreff für die Wurm-Mails aus den Datenbeständen des Wirtsrechners.

> »Viruses and related "worms" typically target computers that run on Microsoft Windows and have a high-speed, always-on connection. In the past six months, a new generation of bug has emerged that contains a so-called Trojan horse program which discreetly installs itself into the innards of the PC
>
> ...
>
> The result is that the computer becomes a "zombie" ready to carry out any nefarious command.
>
> ...
>
> The fast-spreading Sobig.F virus this summer was the first to do this, experts said.«
> ([Reuters 2003b])

### Trojaner

Ein Trojaner ist ein Programm, das sich als etwas anderes ausgibt, um seine wahren Funktionen bzw. Ziele zu verdecken. (vgl. [Wang 2003], S. 87) Dieser wahre Zweck kann auch die eigene Verbreitung umfassen. Hier gibt es vor allem zwei Verbreitungswege, zum einen in Koppelung mit Viren und Würmern. Bekannte Würmer, die einen Trojaner beinhalten, waren kurz vor Verfassung dieser die der Familien MyDoom und Sobig (vgl. hierzu [Delio 2004b] und [Reuters 2003a]).

Einige Trojaner, die spam versenden können, verbreiten sich über peer-to-peer-Netzwerke. (vgl. [Zetter 2004])

> »As it turned out, Sobig's true purpose was to transform infected

> machines into spam-spewing proxy relays that could be secretly used to distribute massive amounts of junk mail.
>
> "It is likely that there's a virus-writer group behind Sobig," said Hypponen. "They used the worm to infect a huge number of computers and then sold various spammer groups lists of proxyservers which would be open for spreading spam. It was clearly a business operation."« [Delio 2003a]

Diese Trojaner installieren auf dem jeweiligen Rechner ein Programm, das Hackern den Fernzugriff ermöglicht. Mit Hilfe des Fernzugriffs werden dann weitere Programme auf den infizierten Rechnern installiert, die andere Rechner zum Beispiel per denial of service Attacken angreifen oder spam versenden:

> »... install a program on the computer to allow the attacker to superrepitiously send spam through it or otherwise take over the machine remotely to speed personal data and files on the computer« [Zetter 2004]

Der Unterschied zwischen Wurm-Mails und Trojaner-Mails besteht darin, dass der Wurm nur durch eine textuelle Nachricht begleitet wird, während beim Trojaner ein komplettes Programm - ggf. mit Aktionen im Sinne von social engineering begleitet - geliefert wird. Die Grenze ist jedoch fließend.

### Spamfutter

Spamfutter entbehrt wie die übrigen Formen des trojanischen spam des eigentlichen semantischen Inhalts, also jeglicher Form einer Nachricht für eine natürliche Person. Ihr Inhalt ist allein dafür bestimmt, die noch näher zu beschreibenden Filter zu irritieren, mit spam Material zu füttern, das ihre Wirkung beeinträchtigt. Zu dem werden auch sinnlose spam verschickt, um zu testen, ob eine Email-Adresse überhaupt existiert. (vgl. insgesamt [Schwartz 1999] und Angebote auf einschlägigen Webseiten, die Software für spamming anbieten[9])

Die Notwendigkeit der Erweiterung der Kategorien von Schwartz und Garfinkel scheint mir im Sinne eines weiten spam-Begriffs deshalb notwendig, da seit 2003 nicht mehr von separaten Erscheinungen gesprochen werden kann. Trojanischer spam stellt nicht mehr nur ein Ärgernis dar, da er als Email eintrifft und wie übriger spam Zeit und Geld kostet. Viren, Würmer und Trojaner können bei ihrer Aktivierung auf einem Rechner weitere Schäden anrichten. Das Neue daran ist, dass sie gezielt eingesetzt werden, um eine Infrastruktur für spammer zu bieten, so zuletzt der Wurm MyDoom [Delio 2004b], oder antispam-Aktivisten zu schädigen [Reuters 2003e] .(siehe auch insgesamt [Delio 2003a] und zu einzelnen Viren/Würmern [Reuters 2003d],

9 z.B. am 4.2.2004: http://www.internetpromotiontool.com/ (Products)

[Zetter 2004])[10]

### *Identifizieren und Filtern*

Bereits in das Internet eingebrachte email spam kann mit Hilfe von Filtern bekämpft werden. Gefiltert werden kann – meist per Software, selten manuell - nach formalen und inhaltlichen Kriterien – gemäß der formalen und inhaltlichen Definition von spam. Spam-Filter kombinieren in der Regel beide Verfahren, zum Beispiel der SpamAssasin.

## Formale Kriterien

Für die Filterung nach formalen Kriterien werden die vier Grundelemente von spam – Absender, Betreff, routing information und Nachrichtenkörper – untersucht und anhand bestimmter Merkmal entschieden, ob es sich bei einer Email um spam handelt oder nicht. Handelt es sich um spam, so wird diese aussortiert oder sogar direkt gelöscht. Wie bereits dargelegt wurde, genügt nicht allein die Identifiaktion einer mail als spam, sondern es muss auch definiert werden, was keine spam ist. Bezüglich der Absenderangaben erfolgt dies anhand sogenannter blacklists bzw. whitelists. Wie diese Listen zustande kommen ist nun entscheidend. Für ihre Erstellung ist die Betrachtung des gesamten Email-Verkehrs, eines großen Ausschnitts, wie die gesamte Post auf einem Server, oder zumindest des gesamten Emailverkehrs eines Anwenders. Dies stellt einen immensen Arbeitsaufwand dar. Eine Reduzierung ist durch die Kooperation mit anderen Anwendern und Automatisierung möglich. Mehrdeutigkeiten bei der Interpretation und Täuschungsversuche der spammer erschweren die Identifikation.

## Inhaltliche Kriterien

Filtern nach Kriterien der inhaltlichen Definition von spam erfolgt mit einer Analyse des Nachrichtenkörpers. Am weitesten verbreitet sind derzeit so genannte Bayes-Filter und selbstlernende Filter, die die Markierung von spam als solche und die Korrektur fälschlicher Weise als spam aussortierter spam (false positives) durch den Nutzer auswerten. Diese Filter berechnen anhand verschiedener Merkmale der eingehenden Emails die Wahrscheinlichkeit, dass es sich um spam handelt.

Der große Vorteil für den Nutzer besteht darin, dass er keine blacklist und whitelist erstellen muss, sondern die Filter seine Entscheidungen, was spam ist, erlernen. Für die Anwendung ist es wichtig, dass der Nutzer dem Filter mitteilt, ob er eine Email

10 Auf eine Schilderung des negativen Einflusses von spam, Viren, Würmern und Trojanern auf die Sicherheitswerte der IT-Sicherheit (vgl. [Winkel 2000]), der die Akzeptanz der IuK-System verringert, wird in dieser Arbeit verzichet.

gelöscht hat, weil er sich nicht mehr braucht oder weil es sich um spam handelt. Diese Filter bieten vom Konzept her auch eine Lösung für das Problem der unterschiedlichen Definition von spam an, da sie die Definition des Nutzers übernehmen. So können derartige Filter erlernen, unangefordert zugesandte Emails mit politischen Inhalt nicht als spam auszusortieren, falls dies dem Nutzerverhalten entspricht.

Die Erfolgsquote bezüglich der Filterung von spam ist bei Filterung nach inhaltlichen Kriterien höher als bei formellen Kriterien, auch wenn hier ebenfalls Beeinträchigungen durch die spammer versucht werden, in dem z.B. täuschende Texte – Spamfutter - mitgeschickt werden. Die Filter nutzen, dass je nach Interessen und Beschäftigung des Nutzers, sich die Themen seiner Emails von denen anderer Nutzer unterscheiden. Dennoch taucht auch hier das Problem der false positives auf. Dies hat – zumindest für die englischsprachigen Nutzer – bereits Rückwirkungen auf ihr online-Verhalten, da bestimmte Worte und Phrasen in Emails vermieden werden, wenn sie die Wahrscheinlichkeit der fälschlichen Filterung der eigenen Email erhöhen (vgl. [Delio 2004a] und [Delio 2003c]). Insbesondere sind Merkmale und Themen betreffen, die häufig in spam vorkommen. (vgl. Austellung auf Seite 13, [FTC 2003]). Eine Selbstzensur findet statt. Da per spam häufig spam- und antispam-Software beworben wird, sind hiervon zum Beispiel auch regelmäßig Emails von antispam-Aktivisten betroffen (hierzu insbesonders [Delio 2004a])

Einige Autoren vermuten, dass das Problem der false positives insbesondere daher rührt, dass die Inhalte der Postfächer von Programmierern einfacher strukturiert sind, als die von Nutzern, die Beschäftigungen jenseits der IT-Branche nachgehen [Baard 2004]. Diese These von Terry Sullivan, einem Mitglied der Antispam Research Group, deckt sich mit der Vermutung von Craig Hughes, Chefarchtitekt bei McAfee Security und Mitentwickler der Filtersoftware SpamAssasin, das bessere Erfolge bei der spam-Filterung auch sozioglogische Nebeneffekte erzeugen werden [Delio 2004a]. Die Filtertechnik sei daher durch die Umstände, unter denen sie entstanden ist, vor allem für im IT-Bereich Tätige geeignet.

Einige Informationen über spam sind nur durch den Vergleich der Posteingangsordner mehrerer Nutzer, zum Beispiel aller eines Netzwerks oder des gleichen Emailservers, erhältlich. Zur Verbesserung der Filtertechnik ergibt sich die Notwendigkeit, die Filter miteinander kommunzieren zu lassen und Filtertechnik auch bereits am Server anzuwenden. Filtertechnik in Servern verringert beachtlich den Arbeitsaufwand für clients (Rechner der Nutzer) und die Nutzer, entzieht ihnen aber auch Entscheidungs- und Eingriffsmöglichkeiten. Dies kann bei der Löschung von als spam identifzierten

Emails und sogenannten false positives rechtliche Konsequenzen haben, so dass einige Provider sich auf das Markieren von spam beschränken[11], diese in spezielle Ordner verschieben[12] und Haftungsausschlüsse in ihren AGB vornehmen. Dem Risiko der false positives stehen die Ersparnisse an Zeit und Geld gegenüber.

## false positives

Aufgrund der Existenz von false positives tauchen Regeln einer Netiquette auf, die beschreibt, welche Wörter und Phrasen in Emails nicht benutzt werden dürfen. Als Beispiel sei hier die Verwendung des Wortes *opt* in Verbindung mit *in* und *out* genannt, das von vielen Filtern als Erkennung für spam benutzt wird, seit dem nach dem seit 1.1.2004 für die USA geltenden CAN SPAM act spam mit einem remove request versehen sein muss, der dem Empfänger die Möglichkeit des opt-out von weiteren Emails bietet. Wie das Kürzel „ADV“ im Betreff weist opt-out im Nachrichtenkörper – insbesondere an seinem Ende – auf eine spam hin. Auch aufgrund des Phänomens von Werbung für spam und antispam-Software per spam ist das Thema „spam“ selber ein Filterkriterium. Es findet inzwischen eine Selbstzensur bei spam-typischen Themen statt, da ihre Erwähnung die Wahrscheinlichkeit des Filterns erhöht. (vgl. insgesamt [Delio 2004a], zur Problematik der „ADV“-Kennung siehe [Delio 2003f])

Versender von regulären Marketing-Mails, die von Nutzern bestellt wurden, beklagen ebenfalls, dass ihre Emails nicht durch Filter durchgelassen werden. Im Oktober beklagte Assurance Systems, dass der Anteil dieser falsch gefilterten Emails bei mindestens 12% und höhere Geschäftseinbußen mit sich bringe würde. Teilweise testen die Versender ihre Emails oder lassen von anderen testen, ob diese durch die Filter schlüpfen. Besteht die Gefahr, dass sie durch Filter gelöscht werden, so passen die Werber ihre Emails an. Eine Verbesserung der Filtertechnik stellt eine Lösung für die false positives dar. Craig Hughes, Chefarchtiekt bei McAffee Security und Mitentwickler des SpamAssassin geht davon aus, dass es zu einer weiteren evolutionären Weiterentwicklung der Filter kommen wird – ähnlich einem Katz- und Mausspiel;

> "If you consider the problem as being a dynamic, evolving system in which spammers, nonspammers and antispammers are all shifting to stay alive in the evolutionary landscape, the precision and sensitivity of the filters will likely oscillate over time -- barring the extinction of either spammers or nonspammers," [...]
>
> "The stratification of e-mail users," he added, "both senders and recipients, due to these Darwinian pressures will be an interesting phenomenon to watch in the coming years. Unfortunately it looks like

11 Zum Beispiel <? SPAM ?>-Markierung im Bereich der Server der JLU Gießen
12 Zum Beispiel web.de

it'll be pretty miserable for those at the bottom of the pile." [Delio 2004a]

Wie die inhaltliche Definition von spam für wenig produktiv gehalten wird, wird auch das Filtern nach inhaltlichen Kriterien für weniger produktiv gehalten. Die großen Erfolge der Bayes'schen Filter täuschen, da das Problem der false positives nicht gelöst ist. Die OECD weist in ihrer Studie auf die Grenzen einer Filterung hin ([OECD 2004], S.29f). Eine Schlussfolgerung kann sein, dass mehr und bessere formelle Kriterien benötigt werden.

### "Wegen des Spams lese ich eh keine Mails mehr."[13]

Spam beeinträchtigt die weitere Verbreitung der Anwendung Email zu einem Zeitpunkt, bei dem breitere Massen an Nutzern erschlossen werden könnten. Für viele netznahe Gruppen, zum Beispiel Studenten und Politiker[14], ist der Email-Dienst nicht mehr weg zu denken. Email als Killerapplikation des Internets ist dabei, netzferne, weniger technik-enthusiastische Gruppen für die Nutzung zu gewinnen. Kamen die technikbegeisterten Anwender mit dem spam-Problem zurecht, macht gerade das Wachsen der Nutzerzahlen und somit Inhaber von Email-Adressen spam noch attraktiver. Der Begrifflichkeit von Donald A. Norman nach [Norman 1999], müssen nun die Anwender der Gruppe der frühen Mehrheitspragmatisten gewonnen werden. Die durch ihr Hinzukommen steigenden Nutzerzahlen, machen spam jedoch bezüglich des zu erwartenden Gewinnes attraktiver. Ist es politisch und gesellschaftlich gewünscht[15], den weiteren Einsatz von Email zu forcieren, so ist die weitere Verbreitung gleichzeitig Mit-Verursacher des spam-Problems. [Fallows 2003] zeigt auf (S.7), dass gerade auch das immense Wachstum an spam das Problem verstärkt und die Bekämpfung erst begonnen hat.[16] Der Studie nach werden die Kosten für spam in den USA auf $50 bis $1.400 pro Arbeitsplatz und Jahr, auf 10 bis 87 Milliarden Dollar insgesamt für amerikanische Firmen, geschätzt. (ebenda).

## *spam und Email-Technologie*

Technologien folgen einem Lebenszyklus schreibt Donald A. Norman [Norman 1999] und daher verändern sie sich von ihrer Erfindung bis zum Zeitpunkt allgemeiner Ver-

13 Tomas Jannot, Redakteur von *PC Direkt*, zitiert in [Koser 2004]

14 Für Politiker sei diese erläutert. Insgesamt nimmt die bedeutung des Internets zu. Die kanadische Studie [Kernaghan 2003] belegt dies für kanadische Parlamentarier für alle modernen Informations- und Kommunikationstechnologie. Indirekte Hinweise gibt es durch eine allgemeine Steigerung der Netznutzung von politischen Meinungsführern [Rötzer 2004] und Untersuchungen von traditionellen Medien zum Internet in US.Wahlkämpfen [PEW 2004]

15 So betont der US-Kongress zum Beispiel zu Beginn des CAN SPAM acts die Bedeutung von „electronic mail“ für das Wachstum des Handels.

16 Hier besteht ein Unterschied zur [EU-Studie 2001], die spam für eine Kinderkrankheit des Internets hielt. Dass spam drei Jahre nach dieser Studie weiterhin – und noch umfangreicher – ein Problem darstellt, falsifiziert sie.

breitung. Seiner These nach geht die Computerindustrie weiterhin davon aus, dass sie noch in ihren Kinderschuhen stecke. Es sei aber nun der Zeitpunkt gekommen, dass der Computer und seine Anwendungen eine Wandlung erfahren, die den Bedürfnissen der Kunden gerecht würde und dem Lebenszyklus aller Technologien folge. So würden dann mehr Kunden, Nutzer, gewonnen.

Wie sieht dieser Lebenszyklus aus? Zum einen kann er dadurch beschrieben werden, inwieweit er Bedürfnisse der Benutzer deckt, zum anderen durch die Typen der Benutzer und damit letztlich die Größe des Anwenderkreises. Zunächst zur Abdeckung der Bedürfnisse, dem Entwicklungsgrad einer Technologie:

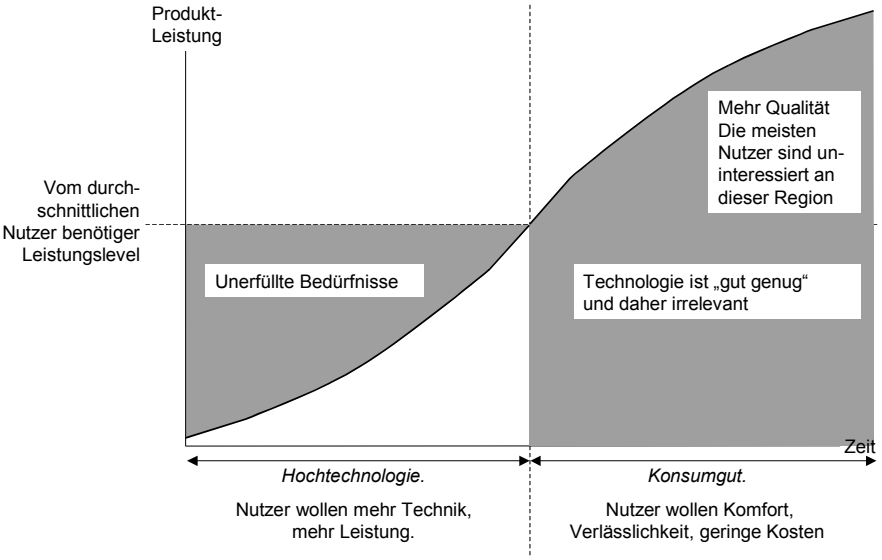


*Abbildung 3 Bedürfnis-Befriedigungs-Kurve einer Technologie, [Norman 1999], S.32*

Zu Beginn liefert eine Technik weniger als der Benutzer erwartet. Mag die Technik noch so unbefriedigend sein und spezielle Kenntnisse in der Bedienung erfordern, so wird sie dennoch eingesetzt, sofern sie ein Bedürfnis des Benutzers erfüllt, wofür er diese Technik benötigt. Trotz aller Schwierigkeiten ist für ihn ein Nutzen erkennbar. Aufgrund der Mängel und dadurch bestehenden Benutzerwünschen wird die Technologie nun verbessert und weitere Funktionen werden ergänzt. Schließlich wird die Technologie "gut genug" sein, um die Bedürfnisse der meisten Benutzer zu befriedigen. Weitere Verbesserungen erhöhen nur noch die Komplexität der Technologie, ohne dass die wichtigen Grundlagen Verbesserungen erfahren.

Mit der fortschreitenden Verbesserung einer Technologie verändert sich auch der Kreis der Benutzer - so insbesondere auch der Käufer. Eine neue Technologie wende

sich zunächst an die Innovatoren, die Enthusiasten, die einfach nach dem Technikeinsatz seiner selbst Willen verlangen. Ihnen folgen die frühen Adaptoren, die Visionäre, die konkrete Anwendungen für neue Technologien sehen. Innovatoren und Adaptoren stellen noch einen geringen Anteil der potentiellen Nutzer einer Technologie, aber sie verhelfen mit ihrem Vorbild sinnvoller Anwendung von Technologie ihr zum Durchbruch, wenn die frühen Pragmatisten den Mehrwert der Technologie und ihrer Anwendungen erkennen. Die Pragmatisten sind dabei bereits nicht mehr an der eigentlichen Technologie, als vielmehr an Lösungen für Probleme interessiert, die durch Technikeinsatz gelöst werden können. Den zweiten großen Anteil der Nutzer stellen die spät folgenden konservativen Nutzer dar. Schlußendlich folgt der Anteil der Skeptiker. Bezüglich der Bedürfnisse der Benutzer zum Zeitpunkt des Durchbruchs einer Technologie tritt eine Veränderung in der Zielsetzung einer Technologie auf. Wird von Anwendungen durch Innovatoren und Adaptoren zunächt überhaupt Technik und Geschwindigkeit erwartet, so wechselt der Fokus durch die Pragmatisten und Konservativen zu Lösungen für konkrete Probleme und Benutzerfreundlichkeit.

Nach Donald A. Norman findet sich die Computerindustrie bereits an diesem Punkt des Durchbruchs. Vielleicht ist sie sogar bereits einen Schritt weiter. Der komplexen Multi-Maschine Computer, die keiner ihrer Anwendungen vollkommen gerecht werden kann, folgen nun Informationsanwendungen, die den Computer in verschiedene Anwendungen auflösen.

> »The PC is maturing from a universally adaptable, "one-size-fits-all" system into a wide range of targeted appliances desgined to solve specific user applications.
>
> - Gordon Moore, cofounder and chairman emeritus, Intel Corporation«
> (zitiert nach [Norman 1999][17])

Email als Killerapplikation des Internets scheint aufgrund der hohen Nutzerzahlen ein Bedürfnis der Nutzer zu decken, auch wenn es meist noch über einen universellen Computer genutzt wird. Spam gehört offenbar aber nicht zu den Bedürfnissen. Spam existiert erst seit den 1990ern, der Email-Dienst hat seine Anfänge in den 1970ern. Nachfolgend sei nun dargelegt, dass der beschriebene Zyklus für den Computer sich auch für den Email-Dienst finden lässt. In diesen Zyklus wird dann das spam-Phänomen einsortiert.

### In welcher Phase befindet sich die Anwendung Email?

Die erste Email wurde Anfang der 1970er Jahre versandt. Es handelte sich um eine

17 Die bei [Norman 1999] angegebene URL mit dem Zitat existiert nicht mehr.

einfache Text-Nachricht im 7-Bit-ASCII-Format. Sie bot weder die Möglichkeit Umlaute darzustellen, noch Dateien anzuhängen.

Normans These der Entwicklung von Technologie folgend wurde die eigentliche Anwendung Email nun im Laufe der Zeit um weitere Funktionen erweitert. Möglichkeiten zur Kodierung von Umlauten wurden entwickelt, schließlich setzte sich hier ein Verfahren um 8-Bit-Daten in 7-Bit-Daten zu verwandeln durch, was schließlich das Übertragen ganzer Dateien ermöglichte. Diese Funktionen, die wir heute weitgehend problemlos benutzen, erforderten aber zunächst spezielle Kenntnisse, um sie zu benutzen. Oftmals verwandelten sich Umlaute und sprachspezifische Zeichen in andere Letter. Auch unterschiedliche Verfahren zur Kodierung von 8-Bit-Daten als 7-Bit-Daten existieren. Inzwischen ist die Kenntnis hiervor irrelevant geworden, die Prozesse wurden automatisiert. Zudem können Emails seit einigen Jahren per HTML formatiert werden, wie auch weitere feature den Dienst und eine Programme komplettierten.

Ich wage hier die These, dass Email-Verkehr auf der Basis eines einfachen Textes der Kern der Anwendung ist. HTML-Formatierung wird verstärkt nur bei Rundmails, Newslettern und gerade auch spam verwendet. HTML macht Email nur komplexer und anfälliger, z.B. für Würmer.

Das unkomplizierte Versenden kurzer Texte und von Dateien scheint der Mehrwert zu sein, der Nutzer im Email-Dienst erblicken.

### Welche Rolle kommt dem Phänomen spam zu?

Email als Technologie befindet sich bezüglich ihres Entwicklungsstandes gemäß der Bedürfnis-Befriedigungskurve im oberen rechten Viertel des Graphen. Zahlreiche Funktionen sind vorhanden, die von den meisten Nutzer weder genutzt noch gebraucht werden. Die Technik ist gut genug, um sich um das eigentlich Technische keine Sorgen zu machen. Allenfalls, wenn Probleme auftauchen, tritt die technische Natur von Email wieder deutlich in den Vordergrund. Dies ist auch der Zeitpunkt, wo die Technik die Kluft zu den frühen Mehrheits-Pragmatisten überschreitet und mehr und mehr Nutzer anzieht. Bei der Anwendung von Email kommt es nun aber bei der weiteren Vermehrung der Nutzer zu dem Phänomen spam. Spam wird erst durch die Ausweitung des Nutzerkreises für die Versender attraktiv. Je mehr Empfänger durch spam erreicht werden können, desto attraktiver wird der. Desto mehr spam-Versender scheint es zu geben und desto mehr spam. Zugleich sind die neuen Nutzer nicht solche, die sich effektiv gegen spam wehren können. Es sind wieder die Technik-Enthu-

siasten und Visionäre, die das Problem früher in Schach hielten und auch nun die ersten technischen Lösungen gegen die spam-Flut einsetzen.

Was zu zeigen war: Die weitere Verbreitung von Email verstärkt das Problem spam, welches erst durch die weiter Verbreitung besteht (siehe auch nachfolgende 'Ökonomie des spam“) und wiederum der weiteren Verbreitung entgegen steht. Die Erfüllung des unerfüllten Bedürfnisses, dass möglichst viele oder alle per Email zu erreichen sind, erzeugt das neue unerfüllte Bedürfnis, dass es kein spam gebe.

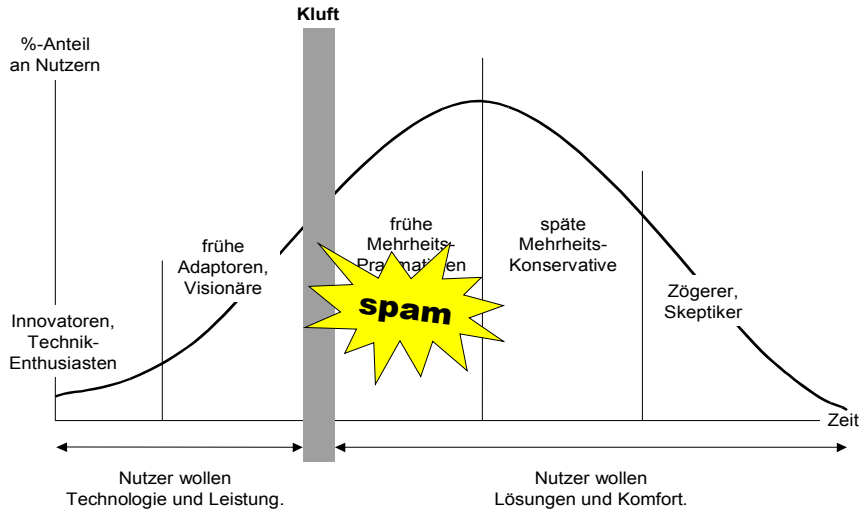


*Abbildung 4 Veränderung der Nutzer bei reifender Technik, nach [Norman 1999], S.33*

## *Ökonomie des spam*

Dass eineVermehrung der Nutzer auch gleichzeitig ein lineares, wenn nicht sogar exponentielles Wachstum von spam zur Folge hat, liegt daran, dass das Versenden von spam derart günstig für den Versender ist, dass von einer Umkehr der Kosten gesprochen werden muss: Nicht der Sender trägt die Kosten dieser Werbung, sondern der Empfänger. Lösungsvorschläge zur Bekämpfung von spam setzen unter anderem daran an, diese Kostenstruktur zu verändern, wodurch es für Marketing uninteressanter werden soll.

> »E-mail may be the cheapest vehicle for direct marketing; costs do not vary according to distance and repeated e-mails have very low additional costs. The very low marginal cost of sending bulk e-mail to individual addresses means that if only one of the addressees becomes a commercial customer, the costs of the particular direct marketing approach can probably be recovered. Therefore, e-mail can be an ideal,cost-effective

> way to build relationships with customers. This also explains why spam is growing at such an alarming rate. Because the costs of sending spam are so low, spammers can make a profit despite extremely low response rates. The more e-mails a spammer can send, the greater the profit, while costs remains nearly constant.
>
> E-mail may be the cheapest vehicle for direct marketing; costs do not vary according to distance and repeated e-mails have very low additional costs. The very low marginal cost of sending bulk e-mail to individual addresses means that if only one of the addressees becomes a commercial customer, the costs of the particular direct marketing approach can probably be recovered. Therefore, e-mail can be an ideal, cost-effective way to build relationships with customers. This also explains why spam is growing at such an alarming rate. Because the costs of sending spam are so low, spammers can make a profit despite extremely low response rates. The more e-mails a spammer can send, the greater the profit, while costs remains nearly constant.«
> [OECD 2004] (S.9)

Die OECD weist in ihrem Bericht zu einer Konferenz über spam Anfang Februar 2004 [OECD 2004] auf einen Fall hin, bei dem 3,5 Millionen spam mails versandt wurden, die innerhalb einer Woche 81 Verkäufe bewirkten. Die Rücklaufquote für diese Akquisition betrug damit nur 0,0023%, dennoch konnte die Firma bei einem Wert von US-$ 19 pro Verkauf einen Gewinn realisieren, selbst wenn sie die Kosten für das spamming übernehmen einzurechnen hat (ebd., S.9).

An dieser Stelle taucht nun erneut die Idee auf, spam zu filtern. Filter-Software soll nicht nur den Nutzer davor bewahren, dass er die spam überhaupt sieht, sondern auch dafür sorgen, dass die Wahrscheinlichkeit, einen Kunden zu gewinnen, massiv reduziert wird, so dass spam nicht mehr attraktiv ist.

> »What the spammers care most about is response rate. In any kind of direct marketing, revenue is proportional to response rate. Spammers are satisfied with a much lower response rate than direct mail, because their cost are so much lower, but response rate is still the key to how much they make. Filtering hits spammers right in their center of gravity: If recipients don't see the spam, they don't respond to it. If we can filter out 95% of spam, we decrease spammers' revenues by a factor of 20. If we can filter out 99.5%, we decrease revenues by a factor of 200. Spammers' costs are low, but not that low. In an article in the Detroit Free Press, one spammer said that he charged a flat fee of $22,000 to send mail to his entire list of 250 million addresses. If filter cut response rates by a factor of 100, the average value of what he was selling would sink to $220. I doubt that would even cover his costs.« [Graham 2003a]

## 2. Politisch-rechtliche Problemstellung

Der erste Teil dieser Arbeit gab einen Überblick, was spam ist und was spam alles sein kann. Eine Typologie von spam ermöglicht verschiedene spam-Arten unterschiedlich zu bewerten und zu bekämpfen. Die Definition von spam ist hierbei entscheidend, da sie bereits den Weg vorgibt. Vielfältig sind die bisher dargelegten Fragen, die im Zusammenhang mit unerwünschten Emails zu lösen sind. Gegliedert ist dieser Abschnitt nach den Phasen, die eine Email von ihrer Entstehung bis zum Empfang durchläuft. Zunächst werden die Empfänger-Adresse und der Inhalt der Nachricht betrachtet. Anschließend folgen Versand, Übermittlung und Empfang.

Der zweite Teil dieser Arbeit verwendet einen engeren Begriff von spam, dieser wird normativ aus einer idealisierten europäischen (EU-)Perspektive entwickelt. Hierbei wird gegenüber einer EU-Studie aus 2001 der Aspekt kommerziell bzw. gewerblich zurückgestellt.[18] Der europäischen Perspektive auf spam wird die us-amerikanische Gesetzgebung gegenübergestellt. Erst zum Ende dieser Arbeit erfolgt ein Übergang dazu, dass es auf der Erde mehr Staaten als die USA und die EU gibt.

Die Einnahme einer europäischen Perspektive liefert die Gefahr, durch die daraus resultierende Strukturierung der Argumente eine europäische Lösung zu präjudizieren. Die Einnahme einer Perspektive stellt jedoch angesichts der Komplexität, der Verschachtelung verschiedener Problemstellungen und stark differierender Definitionen von spam die einzige Möglichkeit einer Strukturierung dar, da eine quasi natürliche Struktur nicht erkennbar ist.

Eine europäische Perspektive wird einer us-amerikanischen bevorzugt, da hier nicht erst die Legitimität des Versands, sondern einen Schritt früher bereits das legitime Sammeln von Email-Adressen thematisiert wird. Dies ist Ausfluss einer unterschiedlichen Tradition, gesellschaftlicher Bedeutung und juristischer Kodifizierung des Datenschutzes. Eine Trennung in eine mehr europäische und mehr (us-)amerikanische Perspektive ist dabei analytischer Natur. Akteure beider politischer Systeme nehmen Positionen ein, die sich offensichtlich im anderen politischen System durchgesetzt haben. Mit Ockhams Rasiermesser wird auf die Betrachtung der Vorgänge im inneren der Akteure USA und EU weitestgehend verzichtet, da ihnen für diese Arbeit kein erklärender Nutzen zukommt.

Vor dem Hintergrund und im Vorgriff der später entwickelten, trivialen These, dass

18 [OECD 2004] (S.7) gibt eine Übersicht zu den „characteristics of spam“, die mit spam assoziiert werden. Auf Grundlage dieser Eigenschaften ließen sich weitere Definitionen entwickeln, jedoch sind „massenhaft“, „unangefordert“ und „kommerziell“ die am häufigsten herangezogenen Eigenschaften.

eine globale Lösung für spam benötigt wird, wundert nicht, wenn die derzeitigen Lösungen in den USA und der EU als Realisierungen von Lösungen unter unterschiedlichen gesellschaftlichen Bedingungen – bei Konstanz der technischen Dimension – interpretiert werden. Eine globale Lösung erfordert entweder eine gemeinsame Lösung oder die Vereinbarkeit unterschiedlicher Lösungen. Bildet das Phänomen spam das gemeinsame Problem, so sind die Definitionen von spam unterschiedlicher Perspektiven Ergebnis unterschiedlicher gesellschaftlicher Rahmenbedingungen und Präferenzen der Akteure beider Regierungssysteme.
Doch nun zu dem hier verwendeten engeren spam-Begriff (siehe Seite 19):

> **»The word "Spam" as applied to Email means Unsolicited Bulk Email ("UBE").**
>
> Unsolicited means that the Recipient has not granted verifiable permission for the message to be sent. Bulk means that the message is sent as part of a larger collection of messages, all having substantively identical content.
>
> **A message is Spam only if it is both Unsolicited *and* Bulk.**
>
> - Unsolicited Email is normal email
> (examples include first contact enquiries, job enquiries, sales enquiries, etc.)
>
> - Bulk Email is normal email
> (examples include subscriber newsletters, discussion lists, information lists, etc.).« [Spamhaus]

Die zwei Kriterien für spam sind a) unerwünschter Empfang und b) massenhafter Versand. Viele Emails werden unverlangt zugesandt. Ein alleiniges Abstellen auf dieses Kriterium würde dem Email-Verkehr unverhältnismäßig erschweren, da immer das Bestehen vorheriger Beziehungen und Email-Komunikation vorausgesetzt würde. Unaufgefordert zugesandte Emails sind häufig und insbesondere zur Herstellung eines Erstkontaktes erforderlich. Politiker haben das Bedürfnis, auch von ihnen bisher persönlich unbekannten Bürgern erreicht werden zu können, wie es Unternehmen nicht akzeptieren könnten, dass ein potenzieller Kunde ohne vorherige Beziehung zum Unternehmen einfach einmal eine Email schreiben dürfte, um zur Abgabe eines Angebotes aufzufordern. Natürlich sind die Rollen von Politikern und Unternehmen besondere, die es eventuell rechtfertigen, dass sie im Gegensatz zu allen übrigen Nutzern des Internets angeschrieben werden dürften. Es käme dann auf den Inhalt der Emails an, die sich auf die Funktion des Empfängers beziehen müsste. Aber mit derartigen Fragestellungen wird eine Diskussion darüber, inwieweit bestimmte Inhalte

spamming erlauben, vorweg genommen. Für eine formelle Definition von spam kann allein das Kriterium herangezogen werden, ob eine vorherige Einwilligung in den Empfang einer Email vorliegt oder nicht. Würde allerdings der Versand nur von Emails statthaft sein, deren Empfang der Empfänger zugestimmt hat, so würde dies den Mehrwert des Email-Dienstes zerstören, einfach und unkompliziert jemandem eine Email zu senden. Wobei ein generelles opt-in für den Empfang allerdings spam insofern verhindern würde, als dass der Versender dem Empfänger auf Grund der Zustimmung bekannt wäre, wenn sich denn alle an die Spielregeln halten würden. Diese Arbeit geht zunächst von dieser idealtypischen Situation aus.

Massenhaft versandte Emails sind im Netz eine regelmäßige Erscheinung. Mailinglisten, die als Diskussionsforum dienen, erzeugen über einen zentralen Server mit einer Email-Adresse ein Instrument, das es erlaubt, über diese Adresse viele Abonnenten dieses Dienstes zu erreichen. Desgleichen gilt für sogenannte Newsletter, bei denen in der Regel sich nur einer an alle Abonnenten wendet. Von spam unterscheiden sich die Newsletter gerade dadurch, dass der Empfänger den Empfang wünscht (opt-in) und diesen Wunsch entsprechend geäußert hat.

| *Email* | **Einzeln** | **Massenhaft** |
|---|---|---|
| **Angefordert** | „normaler“ Email-Vekehr zwischen gegenseitig bekannten Teilnehmern | Mailingliste, Newsletter |
| **Unangefordert** | Erst-Kontakt | spam |

*Tabelle 5 Kriterien für spam*

Vielfach wird spam mit kommerziellen bzw. gewerblichen Inhalten verbunden. Der Abschnitt der EU-Studie mit dem Title „Different concepts of unsolicited commercial e-mail“ beginnt, mit einer Defintion von unangefordert und kommerziell. Hier wurde als zweites Kriterium anstatt massenhaft, das inhaltliche Kriterium „kommerziell“ herangezogen:

> »Strictly speaking, an unsolicited commercial communication has two essential characteristics: its commercial nature and the fact that it is unsolicited i.e. not requested in advance by the Internet user.« [EU-Studie 2001], S.38

Eine Definition von spam über dieses Kriterium stellt wieder einen inhaltlichen Aspekt dar und wird daher verworfen. Die Diskussionen, ob kommerzielle und massenhaft versandte Email – Werbung – zulässig sind, wird auf später vertagt, ebenso wie die Diskussion, wie es um Werbung für ein Produkt oder eine Dienstleistung

steht, bei dem sich ein Unternehmen gezielt nur an einen oder wenige Teilnehmer wendet. (siehe Seite 46)

„Einen oder wenige“ gibt hier das Stichwort für ein Problem der dargestellten Tabelle 5. Die Unterscheidung zwischen angefordert und unangefordert stellt sich, wenn nur formale Kriterien herangezogen werden, als einfach dar. Eine Definition von „massenhaft“ stellt sich als schwieriger dar. Kann bei mehr als einem Empfänger bereits von massenhaften Versand gesprochen werden? Ab wieviel Empfängern kann von massenhaften Versand gesprochen werden? Diese Frage kann hier nicht beantwortet werden. Die Antwort hierauf wäre durch die Gesellschaft zu geben und vom Gesetzgeber zu kodifizieren. Die Abgrenzung von massenhaft zu nicht-massenhaft – in der Tabelle als „einzeln“ benannt – ist gerade ein Regulierungselement, das dem Gesetzgeber zu Verfügung steht. So könnte die Grenze von legitimer Email zu spam durch eine weitere Drosselung der Grenze für „massenhaft“ reguliert werden. 1.000 Empfänger dürften einen massenhaften Versand darstellen, bei 100 ist es noch zu vermuten, eventuell auch weniger. Eine Einschränkung für legitime Newsletter und Mailinglisten darf hingegen hierdurch nicht begründet werden.

Außer der Zahl der Empfänger dürfte für diese Grenze aber noch weitere Kriterien hinzukommen, wie zum Beispiel eine Gruppenzugehörigkeit. Hier wäre eine Email an 603 beliebige Empfänger bezüglich des Kriteriums „massenhaft“ anders zu bewerten als eine Email an die 603 Mitglieder des Deutschen Bundestages. Fraglich wäre hier, ob sich eine derartige Email an die Mitglieder des Deutschen Bundestages auf ihre Rolle als Abgeordnete beziehen würde, wofür wieder inhaltliche Kriterien heranzuziehen wären.

Spam im engeren Sinne sei eine unaufgefordert, massenhaft versandte Email (UBE).

### *Adressen*

Die Zulässigkeit des Versands ließe sich gerade zum Zeitpunkt des Versendens, der Initiierung des Versands, prüfen. Falls es sich um eine Email mit hinreichender Anzahl an Empfängern handelt, dass von massenhaften Versand gesprochen werden kann, dann muss geprüft werden, ob jeder einzelne Empfänger dem Versand zugestimmt hat. Ist dies nicht der Fall, dann handelt es sich um spam im engeren Sinne.

In der Zustimmung zum Empfang unterscheiden sich die europäische von der amerikanischen Perspektive. Stellt die amerikanische Perspektive darauf ab, ob es zulässig ist, dem Inhaber der Email-Adresse die vorliegende Email zuzustellen, so stellt die europäische Perspektive die Frage, ob es überhaupt zulässig sei, dass der Versender

die Email-Adresse kennt, und unter welchen Umständen es ihm gestattet ist, diese zu speichern und gegebenenfalls zu nutzen. In amerikanischer Perspektive liegen Adresse und Nachricht vor. Anhand der Nachricht wäre dann – also mehr inhaltlich – zu prüfen, ob ein Versand zulässig ist. In dieser Perspektive kann unterschiedlich betrachtet werden, ob die Email-Adresse selber und die Art und Weise, wie sie dem Versender zur Kenntnis kam, eine Rolle bei der Feststellung der Zulässigkeit des Versands spielen.

Der Unterschied zur europäischen Perspektive ist gravierend. Hier findet zunächst die Prüfung statt, ob der Besitz der Kenntnis einer Email-Adresse überhaupt statthaft ist. Diese Kenntnis ist mit einer Zweckbestimmung verbunden, die bereits die Zulässigkeit des Besitzes, ihre Speicherung zur späteren Verwendung, begrenzt. Weiterhin hat die Zweckbestimmung einen Einfluss darauf, ob die Email bezüglich ihres Inhaltes als angefordert oder nicht–angefordert gilt, der Versand also im Rahmen der Zweckbestimmung erfolgte.

Die Email-Adressen fürs spamming werden entweder selber aus öffentlichen Bereichen des Internets gewonnen oder von Dienstleistern, die gerade dies gemacht haben, bezogen, wenn letzteren nicht sogar die komplette Aktion des spammings übertragen wird.[19] Harvester oder harvesting tools sind Programme, die das world wide web nach Email-Adressen durchsuchen. Einschränkungen hinsichtlich des Inhalts der Seiten oder ihrer Adressen (domain names) sind gängig. (siehe [EU-Studie 2001] , S. 31f) Ähnliche Werkzeuge existieren für das Extrahieren von Adressen aus dem usenet und aus öffentlichen Adressverzeichnissen, denen in Europa jedoch eine geringere Bedeutung zukommt als in den USA. (vgl. [Wang 2003], S.209)

Die [EU-Studie 2001] berichtet von einem Anbieter einer CD-ROM mit 11 Millionen Email-Adressen. Inzwischen liegen derartige Angebote bei dreistelligen Millionen.[20] Über harvester und Dienstleistern können auch Bestände bezogen werden, die mehr oder weniger auf Zielgruppen eingestellt sind. (Eine Übersicht der Zielgruppen hierzu findet sich bei [EU-Studie 2001], S. 37)[21]

Harvester und Adress-Validatoren stellen eine Möglichkeit dar, ohne direkten Kon-

19 [OECD 2004] -( S.10) zeigt eine Übersicht hierzu

20 Es besteht der Verdacht, das zahlreiche Adressen generiert werden, da einige Namen bzw. Namenskombinationen vor dem Klammeraffen (@) häufiger vorkommen.

21 Bei einem Vortrag anlässlich des Chaos Communications Camps 2003 berichtete Christian Mock, Angestellter eines österreichischen ISPs, von dem auftauchenden Phänomen von spam, das bestimmte Sparten bedient, zum Beispiel für australische Surfsport-Ausstatter. Hier werden gezielt Nutzer beschickt, die im Internet zu verwandten Themen gepostet haben, zum Beispiel zu Surfurlaub in Australien. Da dieser spam den Interessen der Nutzer entspricht, ist es schwierig diesen spam zu filtern, der von den üblichen Inhalten gem. [FTC 2003] abweicht. - Die Konferenzmaterialien enthalten nichts hierzu, sie sind unter http://www.ccc.de/camp/2003/conference/ zu finden.

takt mit dem Inhaber einer Email-Adresse in Kontakt zu treten, in die Kenntnis der Existenz seiner Email-Adresse zu gelangen. Der öffentliche Zugriff auf eine Email-Adresse gestattet aus amerikanischer Perspektive die Speicherung, welche aus europäischer Perspektive bereits verboten ist, wenn diese nicht bereits mit der Veröffentlichung bezweckt werden sollte.

## Datenschutz

Der Unterschied zwischen beiden Perspektiven besteht im unterschiedlichen Stellenwert des Datenschutzes in den USA und der EU. In der EU ist Datenschutz Ausfluss der Grundrechte, der Persönlichkeitsrechte der Europäischen Menschenrechtskonvention (EMRK) und der EU-Grundrechte-Charta. Für die Bundesrepublik Deutschland hat das Bundesverfassungsgericht im sogenannten Volkszählungsurteil das Recht auf informationelle Selbstbestimmung aus Artikel 1 (1) des Grundgesetzes entwickelt.[22] Dieses Recht schließt ein, darüber zu entscheiden, wer was über eine natürliche Person wissen darf und zu welchem Zweck diese Informationen genutzt werden dürfen. Da es sich um ein Grundrecht handelt ist der Staat daran gebunden und auch für die Durchsetzung in der Gesellschaft verantwortlich, also auch im Verhältnis zwischen Privaten.

In den USA existiert ein grundrechtlich gesicherter Datenschutz nur im Verhältnis Staat - Bürger. Ein allgemeines Datenschutzrecht existiert nicht (vgl. [EU-Studie 2001], S. 72). Der Datenschutz zwischen privaten Akteuren unterliegt allein ihren privatrechtlichen – zwischen ihnen selbst zu regelnden – Wünschen. Dem Staat kommt hier keine Kompetenz außer der Garantie des Einhalts von Verträgen zu, also der gerichtlichen Sanktion von Verträgen, wenn ein Vertragspartner gegen Rechte und Pflichten eines Vertrages verstößt. Grundsätzlich besteht Vertragsfreiheit. Liegt keine Einschränkung bei der Verwendung von Daten vor, dann ist die Verwendung eher erlaubt als verboten. Personbezogene Daten verlieren so schnell ihre Zweckbindung. Die Zulässigkeit der Speicherung unterliegt keinen datenschutzrechtlichen Einschränkungen. Die amerikanische Perspektive gestattet das Sammeln von Adressen.

In der EU ist bereits die Speicherung personenbezogener Daten, zu denen auch Email-Adressen gehören, an die Zweckbestimmung durch den Inhaber gebunden (opt-in). Die Problematik bezüglich der Daten juristischer Personen sei hier nicht weiter erläu-

22 Auch wenn die gleichen rechtlichen Grundlagen in Deutschland gelten wie in den übrigen EU-Ländern, so erfolgt die Bekämpfung von spam vor Gerichten auf einer anderen rechtlichen Grundlage. Als effektives Instrument taugt hier die Gesetzgebung gegen den unlauteren Wettbewerb. Hieraus haben Gerichte bereits Verbote für unaufgeforderte zugesandte Faxe und Anrufe zu Werbezwecken entwickelt. - vgl. [EU-Studie 2001], S. 86f

tert. Bezüglich der Verfahren in Kenntnis einer Email-Adresse zu gelangen, sei darauf hingewiesen, dass bei einigen Methoden nicht zwischen Adressen natürlicher und juristischer Personen unterschieden werden kann. Einer Email-Adresse ist in der Regel nicht anzusehen, ob sie einer natürlichen oder juristischen Person gehört.

Der massenhafte Versand einer Email bedarf einer Masse an Email-Adressen, die hierfür erfasst und gespeichert werden müssen; in der Regel erfolgt die Speicherung über eine Datenbank, für die weitere besondere gesetzliche Bestimmungen gelten können. Die europäische Perspektive prüft hier bereits die Zulässigkeit der Speicherung, da nach der europäischen Perspektive eine Veröffentlichung dieser – selbst in öffentlichen Diskussionsforen - nicht ihre Zweckbestimmung aufhebt. Die EU-Richtline von 1995 verbietet das Sammeln von Email-Adressen aus öffentlichen Bereichen des Internets. (vgl. [EU-Studie 2001], S.109)

Unangefordert zugesandte Werbung per Email ist seit der UWG Novelle zum 1.1.2004 in Deutschland verboten. Versender von spam können, sofern sie in Deutschland belangt werden können, aufgrund unlauteren Wettbewerbs von Empfängern und Mitbewerbern auf Unterlassung und gegebenenfalls Schadensersatz verklagt werden. Bereits das Sammeln und folglich Speichern der Adressen verstößt ohne Zustimmung der Inhaber gegen das Bundesdatenschutzgesetz.[23]

Befindet sich der spammer außerhalb der Bundesrepublik Deutschland, so ist die Verfolgung nicht so einfach. Bis zur Umsetzung der EU-Richtlinie 2002/58/EG – in Deutschland per UWG-Novelle zum 1.1.2004 – waren in einigen EU-Ländern keine oder andere Regelungen in Kraft.[24]

Erst die in Folge der [EU-Studie 2001] erlassene EU-Richtlinie 2002/58/EG schaffte eine einheitliche Grundlage zum Umgang mit spam und der einheitlichen Beurteilung der grundlegenden „allgemeinen“ EU-Richtlinie 1995/46/EG zum Datenschutz, der EU-Richtlinie 1997/7/EG zum Fernabsatz sowie der Richtlinie 2000/31/EG zum elektronischen Geschäftsverkehr (siehe [EU-Studie 2001], S.100ff); die Richtlinie 2002/58/EG adaptiert und ersetzt die bisherige Telekommunikationsrichtlinie 97/77/EG.

Die EU-Richtlinie 2002/58/EG fordert zwingend von den Mitgliedsstaaten den Erlass von Regelungen, die für zulässige Werbung per Email das opt-in-Modell fordert. In

23 Öffentliche Stellen, die den Landesdatenschutzgesetzen unterliegen, werden hier nicht separat betrachtet, da a) der Anteil spam versendender Stellen, die unter die Landesdatenschutzgesetze fallen, wenige sein dürften und ähnliche Mechanismen und Ziele wie im Bundesdatenschutzgesetz gelten und b) der Fokus auf der Betrachtung des korporativen Akteurs EU.

24 Eine Übersicht hierzu findet sich in [OECD 2004]

Deutschland wurde per UWG-Novelle das vorgeschriebene opt-in-Modell festgelegt. Einige EU-Länder, zum Beispiel die Niederlande, kannten bisher das opt-out-Modell, wie es für die USA mit dem zum 1.1.2004 in Kraft getretenen CAN-SPAM act gilt.

## opt-in vs. Opt-out

Der Hauptkonflikt besteht in der Alternative aus opt-in und opt-out. Opt-out bezeichnet ein Verfahren, bei dem jede spam mail eine Rückantwortadresse oder einen Link enthalten muss, mit deren Hilfe der Nutzer jede weitere spam seitens des Versenders untersagen kann. Opt-in bezeichnet ein Konzept, bei dem der Versand von Emails an jeden verboten ist, der dem Empfang nicht explizit zugestimmt hat. Zu opt-in und opt-out existieren Unterformen. (vgl. [EU-Studie 2001]

| **spam** | **opt-out** | **opt-in** | **confirmed opt-in** |
|---|---|---|---|
| Adressen aus unbekannter Quelle | • Vorhandene Kunden<br>• Keine vorliegende Erlaubnis zur Nutzung der vorhandenen Adressen | Erlaubnis zum Senden von Werbe-Emails wird gegeben | Erlaubnis zum Senden von Werbe-Emails wird gegeben; Nutzer bestätigen Email-Adresse |
| | | | |
| • Kein Ergebnis<br>• Beschwerden<br>• Risko von der Nutzung des Email-Dienstes ausgeschlossen zu werden | • Zahlreiche Beschwerden<br>• nie endende Spirale des opt-out<br>• „Wenn das alle machen würden ...“ | Nicht unfehlbar: Missbrauch fremder Adressen | • Keine<br>• alle Adressen verifiziert<br>• loyale Kunden |
| **Akzeptanz** → | | | |

*Tabelle 6 Von spam zu doppeltem opt-in (nach MessageMedia, in [EU-Studie 2001], S.63)*

Bei opt-in wird zwischen single opt-in und confirmed opt-in – teilweise auch als double opt-in bezeichnet - unterschieden. Bei single opt-in stimmt der Inhaber einer Email-Adresse dem Empfang von Werbemails zu. Mißbrauch ist hier nicht ausgeschlossen, zum Beispiel in Form des „subscription bombing“. Hierbei setzt ein Fremder die Email-Adresse auf zahlreiche Mailinglisten und spam-Verteiler, um dem Inhaber mit der dann zu erwartenden Flut an unerwünschten Emails zu schaden. Da keine Verifizierung der Email-Adressresse oder Authentifizierung des Anmeldenden erfolgt, kann dies beim aktuellen Stand der Technik nicht verhindert werden. Ein weiteres Problem besteht in der Vielzahl an Möglichkeiten, „nebenbei“ einen Newsletter oder eine Mailingliste zu abonnieren, ohne dass dies wahrgenommen wird. Bei zahlreichen Anmeldungen oder Bestellungen auf Webseiten wird so zum Beispiel neben-

bei der Empfang von Emails der entsprechenden Seite oder Firma angeboten. Abhilfe schafft hier das Schema des confirmed opt-in. Auf die Anmeldung zu einem Verteiler bzw. einer Mailingliste folgt hier noch zwingend die Antwort auf eine vom Betreiber – in der Regel automatisch – verfassten Email, die um Bestätigung der Anmeldung bittet. Hierdurch wird bestätigt (confirmed), dass a) die Email-Adresse korrekt eingegeben wurde und b) auch wirklich der Inhaber der Email-Adresse Urheber der Anmeldung ist.

Beim individuellen opt-out Schemata (individual opt-out scheme) ist ein Link oder eine Rückantwortadresse vorgeschrieben, die der Abmeldung – der Generierung eines remove request – dient. Mißbrauchsmöglichkeiten bestehen darin, dass der Link bzw. die Rückantwortadresse falsch ist oder zur Bestätigung der Existenz der Email-Adresse ausgewertet wird. Bei letzterem führt die Auslösung des remove request zu noch mehr spam, da für den spammer die Adresse nun wertvoller ist, da der spam ja offenbar vom Nutzer gelesen wird. Opt-out wird häufig durch sogenannte one time mailings umgangen. Hierbei gibt die spam mail an, dass der Absender nur diese eine Email sende, so dass der Ausschluss weiterer Emails nicht nötig sei, da eh keine folgen würden. Die stimmt oft nicht, da anzunehmen ist, dass der gleiche Urheber oft nur die Absenderangabe verändert. Aber hier tritt auch eine andere Lücke des Verfahrens hervor. Das opt-out schützt nur vor der spam-Flut eines Versenders, hindert ihn nicht an der Weitergabe der Adresse an weitere spammer. Abhilfe hiervon bieten global opt-out-Schemen (in Tabelle 6 nicht dargestellt), die vergleichbar der deutschen Robinson-Liste für Direktmarketingsendungen per gewöhnlicher Post funktionieren. Die Anmeldung einer Email-Adresse bei einer zentralen Registrierungsstelle, die von allen Versendern berücksichtigt werden soll, führt bei diesem Schema zum Ausschluss von sämtlichen Werbungsendungen, von spam.

Für das Funktionieren eines solchen opt-out Schema führt das britische Handelsministerium aus:

> "In order for an opt-out scheme to provide effective consumer protection, it would have to fulfil certain criteria. It would be necessary for:
>
> - all subscribers to be aware of it;
> - it to be simple and free to join;
> - it to become effective within a reasonable time of joining;
> - it to require companies engaged in telemarketing to update their lists regularly in the light of subscribers' notifications;

- it to have adequate complaints handling mechanisms."

  [EuroCAUCE]

EuroCAUCE ergänzt, dass globale opt-out-Schema ohne staatliche Aufsicht und Sanktionen nicht funktionieren können.

Die Mißbrauchsmöglichkeiten sinken von individuellem opt-out, global opt-out, single opt-in zu confirmed opt-in. Parallel steigt der Grad der Akzeptanz für den Nutzer und die Bekämpfung von spam.

Opt-out-Schemen stehen im Widerspruch zu den Prinzipien der EU-Datenschutzrichtline von 1995: dem Prinzip der Zweckbindung der personenbezogenen Daten und das Recht, ihre Verwendung im Voraus zu bestimmen und auszuschließen. Die Preisgabe einer Email-Adresse in einem Diskussionsforum oder zur Abwicklung eines Vertrages auch in Form einer online-Transaktion gestattet nicht die Verwendung in einem anderen Umfeld und für weitere Zwecke. Dies gilt auch bereits für die erste Email mit einem opt-out-Hinweis:

> »By allowing the recipient to register his objection only after the event i.e. after the initial prejudice has been suffered, the opt-out approach deprives Internet users of their rights over their own mailboxes.«
> [EuroCAUCE]

Opt-out Verfahren sind in der Europäischen Union bereits nach der EU-Datenschutzrichtline von 1995 nicht zulässig, da sie die Persönlichkeitsrechte natürlicher Personen verletzen.

Die Studie erklärt die Entscheidung anderer Gesetzgeber für opt-out-Verfahren durch einen geringeren Stellenwert des Datenschutzes in diesen Ländern, was dazu führe, dass zu Gunsten vermeintlicher Ziele eines freien Unternehmertums, das auch das Recht auf Werbung umfasse, die Privatsphäre natürlicher Personen Einschränkungen erfahre. Die [EU-Studie 2001] (S.65) verwirft dies als Verzerrung („distortion“) und unverhältnismäßig, da beim opt-out-Verfahren – wie oben beschrieben – der Inhaber einer Email nur den Empfang von einzelnen Sendern unterbinden, nicht aber die Quelle, die Preisgabe seiner Email-Adresse, unterbinden könne. EuroCAUCE illustriert dies mit einer Beispielrechnung für den Fall, dass bei einem opt-out-Schema nur 1% der Firmen in der EU Email-Werbung versenden würden. Der Inhaber einer einzigen Email-Adresse könnte einen Angestellten bei regulären Arbeitszeiten ein Jahr lang beschäftigen, ihn bei allen Verteilern abzumelden, wobei der Angestellte zwei Abmeldungen pro Minute vorzunehmen hätte.

Opt-out Verfahren sind unverhältnismäßig aufwendiger für den Einzelnen gegenüber opt-in Verfahren.

## CAN SPAM act und EU-Richtlinien

Die amerikanische Perspektive wählt das opt-out-Modell, die europäische Perspektive lässt nur das opt-in-Modell zu, wie es durch die EU-Richtlinie 2002/58/EG verbindlich wurde. Vor dem Hintergrund der bereits existierenden Richtlinien (insbesondere 1995/46/EG) hatte die EU keine andere Wahl, wie es die [EU-Studie 2001] mit dem bezeichnenden Titel „Unsolicited Commercial Communications and Data Protection" darlegt. Die Rechtslage in der EU fasst die OECD wie folgt zusammen:

> »The EU has adopted an "opt-in" approach for commercial communications by e-mail (including SMS), by way of Directive 2002/58/EC of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), which is an integral part of the new, wider EC regulatory framework on electronic communications. Previously, the opt-in was applicable to faxes and automated calling machines.
>
> The Directive contains three basic principles with regard to unsolicited commercial communications. Firstly, according to Article 13(1) of the Privacy and Electronic Communications Directive member states are required to prohibit the sending of unsolicited commercial communications by fax or e-mail or other electronic messaging systems such as SMS and Multi-media Messaging Service (MMS) unless the prior consent of the person has been obtained (opt-in system). This regime is applicable for marketing to individuals (natural persons) but member states can extend the scope to marketing communications to businesses. There is a limited exception from the opt-in system for existing customers [Art 13(2)], for the use of contact details obtained from customers in the context of a sale, but it may only be used by the same legal person for the marketing of 'similar' products or services and provide an explicit opt-out is offered at the time of collection and with each subsequent message. Secondly, the disguise of identity of the sender is prohibited. Thirdly, direct marketing messages must include a valid return address where persons may opt-out ('free of charge and in an easy manner').« ([OECD 2004], S.20)

Innerhalb der EU ist nur das permission based marketing[25] erlaubt. Alle anderen Formen sind unzulässig; die Ausnahme betrifft Artikel 13 (2), der den Mitgliedsstaaten für künftige Formen elektronischer Werbung die Wahl zwischen einem opt-in-Verfahren und einem opt-out-Verfahren lässt. Bezüglich des permission based marketing schreibt die EU-Richtlinie 2002/58/EG zu dem ein verbindliches opt-out per remove request vor. Der CAN SPAM act kennt nur diesen opt-out-Mechanismus

25 auch opt-in e-mail marketing oder permission marketing, zum Begriff vgl. [EU-Studie 2001] - permission marketing ist ein von Yahoo! Urheberrechtlich geschützter Begriff

neben einem geplanten global opt-out-Schema unter Aufsicht der Federal Trade Commission (FTC). Hierzu führt die OECD aus:

> »The United States recently passed legislation on spam, which adopts an opt-out approach. It requires senders of unsolicited commercial e-mail to provide a mechanism to opt-out and requires senders to abide by recipients' requests to opt out. The legislation requires clear and conspicuous disclosure that the message is an advertisement. The senders must include a valid postal address in the e-mail and have a functioning e-mail address.« ([OECD 2004], S.22)

Folgende Argumente zwangen die EU zum opt-in-Schema:

- Eine Abwägung zwischen dem Schutz der Privatsphäre und personenbezogener Daten wie der Email-Adresse gegenüber der Freiheit des Unternehmertums mit einem Recht auf Werbung führten mit Blick auf geltende Regelungen zum Datenschutz zur Wahl des opt-in-Schemas, da bereits eine einzige Email die grundrechtlich gesicherte informationelle Selbstbestimmung, welche das opt-out-Modell bedingen würde, verletzen würde.
- Ein opt-out-Modell erscheint unverhältnismäßig in Hinblick auf den Aufwand, den der Inhaber einer Email-Adresse für die Teilnahme am opt-out-Verfahren betreiben muss.[26] (Beispielrechnung [EU-Studie 2001])

Wie die EU-Studie feststellt, hängt die Wahl zwischen beiden Lösungen vom Stellenwert des Datenschutzes ab. Dieser ist in den USA geringer, Argumente für ein freies Unternehmertum gelten stärker. Der Unterschied manifestiert sich nicht nur gesetzlich, sondern auch in den Präferenzen verschiedener korporativer Akteure, zum Beispiel der Direct Marketing Association (DMA). Diese lehnt ein „opt-in-only regime" (Zitat der DMA nach [EU-Studie 2001], S.30) schon deshalb ab, da sie negative Folgen für legitime Werbe-Emails (permission based marketing) befürchtet.

Die EU wartet mit einem generellen opt-in-Schema auf, dass für jegliche Werbe-Email einen remove request – ein opt-out vorschreibt. Unterschiedliche Regelungen auf nationalstaatlicher Ebene sind innerhalb der EU vorhanden. Spam an Email-Adressen natürlicher Personen ist zum Beispiel in Großbritannien nicht verboten. Da Datenschutz in der EU nur für natürliche Personen einheitlich geregelt ist, ist die englische Lösung Ausfluss nationalstaatlicher Präferenzen. Wie bereits bei den US-Bundesstaaten sei auch hier wieder auf eine Darstellung der Vorgänge innerhalb des Akteuers EU verzichtet. (Eine Übersicht zu Unterschieden zwischen den EU-Ländern

26 Auf Seite 111 erwägt die Studie kurz ein globales opt-out-Register für die EU, das zwangsläufig durch die Wahl von opt-out entstehen müsste. Dies wird als unverhältnismäßig („drakonisch") im Vergleich zur opt-in-Lösung abgelehnt.

findet sich wieder im Anhang von [OECD 2004] und überaltert in der [EU-Studie 2001])

Einige Verwirrung herrscht seit der Einführung auch noch hinsichtlich der weiteren Folgen des CAN SPAM act und nach anderer Auslegung, der Vortäuschung, dass spam mails dem CAN SPAM act genügen würden – einem Verstoß gegen Text und Geist des Gesetzes (siehe [Ulbrich 2004]).

<table>
<tr><th>EU</th><th>USA</th></tr>
<tr><td>opt-in für Werbe-Emails</td><td rowspan="2">( globales ) opt-out</td></tr>
<tr><td>Bestehende Kundenbeziehung als Ausnahme von opt-in</td></tr>
<tr><td colspan="2">Verbergen & Fälschen der Absenderangaben ist verboten</td></tr>
<tr><td colspan="2">korrekte Rückantwortadresse und remove request sind Pflicht</td></tr>
<tr><td colspan="2">klare Identifizierung als Werbung<br>(EU-Fernabsatz-Richtlinie)</td></tr>
<tr><td>Adressbestände zweckgebunden und nur mit Einwilligung der Betroffenen zulässig<br>(EU-Datenschutzrichlinie)</td><td>spamware verboten</td></tr>
</table>

*Tabelle 7 Gegenüberstellung Regelung EU-USA*

Die Gegenüberstellung der Regelungen für die EU und die USA in Tabelle 7 zeigt auf, warum eingangs (Seite 32) von 'idealisierter' europäischer Perspektive gesprochen wurde: Vom verpflichtenden europäischen opt-in-Verfahren gibt es eine Ausnahme bei bestehender Kundenbeziehung. Für diese Werbe-Email gilt wie für das permission based marketing die Pflicht der Aufnahme eines remove requests. Auch muss aufgrund der Fernabsatz-Richtlinie klar sein, dass es sich um Werbung handelt. Hierdurch wird verhindert, das Beworbene scheinbar in eine Kommunikationsbeziehung eingebunden werden, auf deren Basis dann später Werbung zugesandt wird.

### *Inhalte*

Spam hinsichtlich bestimmter Inhalte – ausgenommen bei Verstößen gegen den Jugendschutz oder Straftaten – zuzulassen oder zu filtern, ist jeweils das gleiche Thema, sobald irgend ein Inhalt privilegiert wird. Es wird stets ein a priori Interesse des Empfängers unterstellt, dass er Emails diesen Inhalts bekommen wolle, und dass ein anderer das korrespondierende Recht habe, ihn zu kontaktieren. Für Werbe-Emails war eine entsprechende Abwägung zwischen Datenschutz und vermeintlicher unternehmerischer Freiheit bereits angeführt worden (siehe Seite 41). Für Staaten mit hohem Datenschutzniveau unterstelle ich, dass diese Abwägung stets zugunsten des Datenschutzes ausgeht. Auch für religöse und politische Inhalte wird kein höherwertiges Interesse wie für die unternehmerische Freiheit zu finden sein, das einen Eingriff in das Persönlichkeitsrecht rechtfertigt.

Es finden sich Indizien, dass sich hier wieder die europäische von der amerikanischen Perspektive unterscheidet:

- Aufgrund des geringeren Stellenwertes des Datenschutzes findet sich in den USA spam als Teil von politischen Kampagnen, insbesondere von Mitgliedern des Kongresses [Lee 2003]. Dies wird als legitim angesehen, da „political speech" von der Verfassung geschützt sei und jede Technik ebenso, die diese vereinfache. (siehe [Sweet 2003])
- Das Amtsgericht Rostock hat per Urteil vom 28.1.2003 einem Unterschied zwischen Werbung und politischer „Werbung" widersprochen und auch dem Persönlichkeitsrecht des Artikel 2 Absatz 1 des Grundgesetzes, aus dem das Recht auf informationelle Selbstbestimmung vom Bundesverfassungsgericht abgeleitet wurde, Vorrang vor dem Schutzbereich des Artikel 21 eingeräumt, der Parteien einen Verfassungsauftrag zuweist. Politische Inhalte konstituieren nach Auffassung des Gerichts keine besondere Zulässigkeit der Werbung, auch bei den Emails gleichgestellten E-Cards.

Aus deutscher Perspektive sind politische – und auch analog religöse – Emails kommerziellen gleich gestellt. Ohne opt-in des Empfängers stellen sie spam dar. Weitere Abwägungen betreffend der Unverhältnismäßigkeit eines opt-out-Verfahrens und der Erfordernis eines globalen opt-out-Schemas nicht nur für kommerziellen, sondern auch für politischen und religiösen spam fallen analog zugunsten von opt-in aus.

Die deutsche Perspektive scheint mit der europäischen deckungsgleich zu sein. Derzeit ist nicht zu erkennen, dass dies für eine EU-Land nicht zutrifft. Die EU-Richt-

linie 2002/58/EG ermächtigt in Artikel 12 Absatz 3 die Mitgliedsstaaten jedoch im nicht-kommerziellen Bereich Direktwerbung zwischen eine opt-in und einem (global) opt-out zu wählen. Dies soll in dieser Arbeit nicht weiter berücksichtigt werden.

An dieser Stelle lässt sich nun auch die aufgeworfene Frage beantworten, wann eine Email dem engeren spam-Begriff nach zur spam wird. Die Frage lässt sich dadurch beantworten, dass sie aus europäischer Perspektive irrelevant ist. Aufgrund des starken Schutzes des Persönlichkeitsrechtes, des Datenschutzes, ist jede einzelne Email bereits spam dieser Perspektive, wenn keine Einwilligung in ihren Versand vorliegt. Wie aber angeführt wurde, sind unangeforderte Emails eine regelmäßig Erscheinung. Hilfsweise wird hier dann auf „kommerziell" bzw. im Urteil des AG Rostock auf „Werbung" abgestellt. Allein die Zweckbindung beim Kenntniserlang von einer Email-Adresse definiert die Zulässigkeit eines Versands.

Gegenüber spam im engere Sinne betont die europäische Perspektive ausschließlich das Kriterium unangefordert. Nicht angeforderte Emails sind spam. Weiterhin müssen kommerzielle Emails einige Anforderungen erfüllen.

In der amerikanischen Perspektive stellt die Menge aber auch kein Kriterium dar.[27] Auch hier wird wieder allein auf das Kriterium „unangefordert" angestellt, wenn auch zunächst angenommen wird, dass eine Email solange als angefordert gilt, bis dieser unterstellten Zustimmung widersprochen wird. Um diesen Widerspruch zu vereinfachen, wird das Konzept des global opt-out eingeführt.

Die Definition von spam im engeren Sinne („UBE"), aus europäischer und amerikanischer Perspektive fallen auseinander. Die beiden letzten fokussieren allein das Kriterium „unangefordert". Zwar werden formelle Kriterien wie unverfälschte Absenderangaben durch die gesetzlichen Regelungen gestärkt, aber kein Äquivalent für das Kriterium „massenhaft" bisher angboten. Dies ermöglicht Dritten außerhalb der Beziehung Sender-Empfänger nicht anhand einer oder mehrer Emails zu beurteilen, ob es sich bei einer Email um spam der jeweiligen Perspektive handelt. Für die Welt der ISPs stellen sich die spam-Definitionen beider Perspektiven als weltfremd dar.

### *Versand*

Die amerikanische Perspektive widmet sich dem legitimen Versand von Emails. Die Rechtmäßigkeit des Versendens in Hinsicht der zu einer Email-Adresse gehörenden

27 Ansätze finden sich bei den Strafbestimmungen („PENATLIES", „FORFEITURE") des CAN SPAM acts. Hier heißt es zum Beispiel:
*"(3) MULTIPLE.—The term 'multiple' means more than 100 electronic mail messages during a 24-hour period, more than 1,000 electronic mail messages during a 30-day period, or more than 10,000 electronic mail messages during a 1-year period."*
*(CAN SPAM act of 2003, section 4)*

Zweckbindung, die nur in europäischer Perspektive existiert, ist, wie vorher dargelegt wurde, nicht unbedingt gegeben. Der CAN SPAM act schreibt, wie ebenfalls schon dargelegt wurde, die Korrektheit der Absenderangaben und einen verbindlichen opt-out-Mechanismus (remove-request) vor.

Ebenso wie der Ansatz, spam per „ADV"-Kennung im Betreff kenntlich zu machen, verletzt die Aufnahme eines remove requests eventuell das Recht der positiven Redefreiheit. Das positive Recht auf Redefreiheit verbietet es, Reden, Texte und Emails zu unterdrücken und zu zensieren. Dieses Grundrecht wird pro spam ins Feld geführt, in dem behauptet wird, ein Verbot von spam wäre ein Eingriff in die Redefreiheit. Ebenso wäre der Zwang zur Aufnahme der „ADV"-Kennung in den Betreff ein Angriff auf die Redefreiheit. Hier wird argumentiert, dass Redefreiheit nicht nur generell die Email an sich betreffe, sondern dass auch nicht vorgeschrieben werden dürfe, welche Inhalte sie haben muss bzw. ebenfalls umfassen muss. Ein Hinweis auf einen remove request stellt in diesem Sinne ebenso einen Eingriff in die posiive Redefreiheit[28] dar, wie eine „ADV"-Kennung. (zur geringen Verwendung siehe [FTC 2003])

Diese Position bedarf der Abwägung mit den Interessen der Empfänger von spam. Redefreiheit mag gegeben sein, es besteht jedoch kein Zwang zum Zuhören. Niemand kann gezwungen werden, Emails zu lesen. Abzuwägen wäre, inwieweit bereits die Zustellung bzw. die Nicht-Zustellung zulässig wäre.

Angemerkt sei, dass ein dargestellter Eingriff in die negative Redefreiheit das Filtern von Emails erleichtert, da zusätzliche formelle Merkmale, zum Beispiel die „ADV"-Kennung, herangezogen werden können. Rein formelle Bestandteile sind ggf. wiederum kein Eingriff in die Redefreiheit. Wie auch immer: Mit dem Erlass des CAN SPAM acts ist die Diskussion um die „ADV"-Kennung obsolet geworden, da sie einheitlich für alle Bundesstaaten der USA nicht mehr vorgeschrieben ist.

Der CAN SPAM act kennt nur die genannten formalen Kriterien. Er erklärt spam mit falschen Absenderangaben für unzulässig. Dieser rechtliche Ansatz gleicht der technischen Lösung, die AOL zum Januar 2004 unter dem Namen „Sender Permitted From" (SPF-Erweiterung für das SMTP-Protokoll) einführte. [Baard 2004] berichtet vom antispam- und open-dource-Aktivisten Eric Raymond, der sich für SPF einsetzt:

> »Raymond is promoting an antispam technology called SPF (sender permitted from), an open-standard SMTP (simple mail transfer protocol) extension that stops spam before ISPs have to download messages by

28 Positive Redefreiheit bezeichnet das postive Recht zu sagen, was einem beliebt, die Nichteinmischung in das, was gesagt wird. „ADV" schreibt gerade vor, das die in den Inhalt einer Nachricht aufgenommen wird – sofern dies nicht als ein rein formelles Element angesehen wird.

> rejecting those e-mails coming from forged addresses. Under SPF, e-mail users enter their valid domains and IP addresses into the SPF registry. More than 4,000 domains have published their SPF records, including AOL, said Raymond. The registry will also be supported by an upcoming version of SpamAssasin and other antispam applications.
>
> SPF is one of the methods that developers presented at the conference for creating so-called "whitelists," lists of approved e-mail senders that enable e-mail recipients to welcome messages from those who are on the list while flagging or rejecting others.
>
> Whitelists like SPF will complement other technologies, such as domain blacklists that block out specific senders, by forcing spammers to use their own domains, said Raymond.
>
> "We need more approaches like SPF that attack the problem further upstream, by forcing spammers into the open," he said.«
> (vgl. auch [Fischer 2004])

Erst eine Verifizierung des Absenders erleichtert den (automatisierten) Aufbau von whitelists – und auch trusted systems -, die als Kriterien zur Filterung von Emails herangezogen werden können.[29]

Einige behaupten, der CAN SPAM act ermögliche erst spam, da er die Filterung verhindere und SPAM legitimiere. (siehe z.B. antispam-Forscher und -Entwickler William Yerazunis in [Asaravala 2003a] ) Das Wortspiel mit der Abkürzung und dem englischen Verb für „können“ – to can – ist offensichtlich. Die Befürchtung besteht darin, dass angenommen wird, spam sei legitim, wenn es die Kriterien des CAN SPAM act erfülle. Dies trifft nur zum Teil zu. Der CAN SPAM act regelt zahlreiche Aspekte bundeseinheitlich – so auch, welche bundesstaatlichen Regelungen bestehen bleiben, welche durch den CAN SPAM übergangen („supersedes“) werden. Unkenrufe, dass er spam gar nicht bekämpfe, sind auf übersteigerte Erwartungen im Zusammenhang mit der Verabschiedung des Gesetzes durch US-Kongress und später die Unterzeichnung durch US-Präsident Georg W. Bush am 16. Dezember 2003 zurückzuführen. Die Berichterstattung über den CAN SPAM act wandelte sich von Dezember 2003 zu Januar 2004 - vergleiche zum Beispiel [Reuter 2003e], [AP 2003d], [AP 2003e], [AP 2003f] mit [Asaravala 2004], [Delio 2004a]. Die Hoffnung war, dass er spam kurzfristig erfolgreich bekämpfe, was sich bereits einen Monat später als falsch heraus stellte. [Delio 2004a] Der CAN SPAM act war auch nicht zur direkten Bekämpfung von spam ausgelegt. Er vereinheitlicht einige Voraussetzungen zur erfolgreichen Bekämpfung durch die Bundesstaaten und regelt Strafverfolgung und Straf-

29 (zur Problematik der trusted systems sei auf insgesamt auf [Lessig 1999] verwiesen, auch wenn sich seine Ausführungen auf das Urheberrecht, nicht auf spam, beziehen

maß einheitlich.

Um spam zu sanktionieren, muss der spammer zunächst identifiziert werden. Die Verhinderung dieser Identifizierung, das Vertuschen des Absenders, stellt gemäß CAN SPAM act einen strafbewährten Verstoß dar. Dies soll vor allem die Versender von betrügerischem spam bekämpfen. Das Vertuschen der Absenderangaben und das Vortäuschen eines anderen Absenders sind zudem auch Methoden, die spammer anwenden, um Email-Server und antispam-Software, wie zum Beispiel spam-Filter, zu überlisten. Dies steht nun unter Strafe: nicht nur das Ausweichen vor der Strafverfolgung, sondern auch das Manipulieren von Servern und Filtern durch falsche Absenderangaben. Der Missbrauch fremder Computersysteme (hacking) ist bereits strafbewährt.
Remove requests und global opt-out-Schema bringen Erleichterung für die Inhaber von Email-Adressen. Das Nicht-Beachten der Regel wird sanktioniert. Alle drei Regelungen sind in den USA seit dem 1.1.2004 bundeseinheitlich geregelt. Die Strafverfolgung erfolgt durch die FTC, aber auch durch die Staatsanwaltschaften der Bundesstaaten, die ergänzend eigene Gesetze erlassen können. Dies ermöglicht die Weiterentwicklung von antispam-Gesetzen im Rahmen eines föderalen Wettbewerbs.

Der CAN SPAM act legt einige formelle Regeln für den Versand von spam fest. Ers stärkt die Kriterien einer formellen Definition, da ein Verstoß gegen die Regeln bereits strafbewährt ist.

Auf eine Darstellung der Gesetze einzelner amerikanischer Bundesstaaten wird hier gemäß Ockhams Rasiermesser verzichtet, da den Erfahrungen und Prozessen im Vorfeld des CAN SPAM acts hinsichtlich der Konstellation und Präferenzen der Akteure USA und EU keine große Bedeutung mehr beigemessen wird. (Die [EU-Studie 2001] , die zeitlich deutlich vor dem CAN SPAM act entstand, gibt einen Überblick, während sich die OECD-Studie [OECD 2004] bereits – wie weiter oben zitiert – ebenso beschränkt.)

## Implementation des global opt-out-Systems

Zu ergänzen ist noch, dass die USA mit dem CAN SPAM act auch den Aufbau eines global opt-out-Verfahrens unter dem Dach bzw. der Überwachung der FTC anstreben[30]. Für ein global opt-out-Verfahren führt EuroCAUCE die vorgenannten Bedingungen auf, die hier erfüllt zu sein scheinen. Mit dem Aufbau ist gemäß dem im CAN SPAM act vorgegebenen Zeitplan nicht vor Herbst 2004 zu rechnen (sieh CAN SPAM act und [Asaravala 2004]). Der Erfolg dieser Institution ist abzuwarten. Diese

30 Der CAN SPAM act nennt es „nationwide marketing Do-Not-E-Mail registry“.

Arbeit geht zunächst davon aus, dass ein global opt-out-Verfahren technisch machbar ist. Zur Realisierungen und Problemen eines global opt-out-Verfahrens hat der US-Kongress von der FTC einen Bericht eingefordert, der laut Zeitplan im CAN SPAM act zur Jahresmitte 2004 vorzulegen ist.

Abzuwarten ist betreffend der amerikanischen Perspektive, ob ein global opt-out-Verfahren erfolgreich ist. Für 2004 ist mit geringen Sanktionen zu rechnen, da die zuständigen Staatsanwälte bekunden, nicht hinreichend finanzielle Mittel zur Verfügung zu haben für den CAN SPAM act, der im Moment nur Verstöße gegen das individuelle opt-out ahnden läßt. (siehe [Ulbrich 2004]) Dies kann auch daran liegen, dass der CAN SPAM act erst im Dezember 2003 von US-Präsidenten Georg W. Bush unterzeichnet wurde, als die Budgetplanungen für 2004 schon abgeschlossen sein dürften. Das Weiterführen von Ermittlungsverfahren auf Grundlage bisheriger bundesstaatlicher Gesetzgebung bleibt unberührt.
Für die Implementation des global opt-out-Schemas stelle ich die These auf, dass Verstöße verstärkt verfolgt werden, da sich dies betreffend des global opt-out-Schemas einfacher umzusetzen sein wird als ein Verstoß gegenüber einem einzelnen Nutzer. Die These wird dadurch bestärkt, dass der CAN SPAM act das Klagerecht in den Händen der FTC konzentriert.

Diese Konzentration wird jedoch auch kritisiert betreffend eines (bisher) fehlenden Verfahrens [Glasner 2004], die FTC auf Verstöße aufmerksam zu machen, und keinen Klageweg für Nutzer vorzusehen. [Asaravala 2004] Da das Verbot von Emails mit falschen Absenderangaben nicht grundrechtlich bedingt ist, war ein entsprechendes Klagerecht für einzelne Bürger nicht zwingend. Ein Verstoß liegt allenfalls auf privatrechtlicher Basis vor, wenn durch spamming gegen vertraglich zugesagten Datenschutz verstoßen wird, was auch unlauteren Wettbewerb, für dessen Verfolgung in den USA die FTC zuständig ist, darstellen kann. Unlauterer Wettbewerb läge dann vor, wenn ein Unternehmen vorgibt, personenbezogene Daten nicht weiterzugeben, aber dennoch Email-Adressen an spammer weitergibt.

Ein Verbot der Sanktionierung durch Private kann aber auch als Zeichen dafür gewertet werden, dass dem global opt-out-Verfahren der FTC die eigentliche Bedeutung beigemessen wird.

Im Falle der erfolgreichen Implementation des global opt-out-Verfahrens ergibt sich für die USA ein System, das für jede einzelne Werbe-Email zusätzlich einen remove request – ein einfaches opt-out vorschreibt. Das global opt-out- stellt gegenüber einem opt-in-Schema einen Kompromiss zwischen Interessen des Datenschutzes, höheren

Ansprüchen an die Redefreiheit (free speech) und der unternehmerischen Freiheit dar.

Es darf gehofft werden, dass sich mit der Implementation des global opt-out-Schemas auch die Ökonomie von spam verändert: Zum einen kann erwartet werden, dass bereits bei der Durchsetzung des opt-out-Schemas und formeller Kriterien, wie zum Beispiel remove request und unverfälschte Absenderangabe, Gewinnabschöpfungen und Strafen (s. [Delio 2004a], [Delio 2003d]) das Risiko der spammer erhöhen und den Gewinn verringern. Zum anderen ist zu hoffen, dass die Akzeptanz des global opt-out-Verfahrens bei erfolgreicher Implementation derart groß ist, dass die Rücklaufquote wie durchs Filtern weiter abnimmt, so das weniger Gewinne realisiert werden können. Dies könnte eine weitere Hinwendung zum permission based marketing oder eine Spezialisierung auf spezielle Nutzergruppen bewirken.

## opt-in und opt-out

Amerikanisches global opt-out-Schema und europäische opt-in-Lösung lassen sich in einem Internet ohne Grenzen miteinander vereinbaren. Zwingend erforderlich ist jedoch, dass die Implementation des global opt-out-Schemas gelingt.

Eine Voraussetzung für die Vereinbarkeit ist, dass auch europäische Nutzer am global opt-out-Verfahren der FTC teilnehmen dürfen. Aus europäischer Perspektive ist nicht akzeptabel, dass ein opt-out jeder einzelnen Adresse durch ihren Inhaber nötig ist. Die Beispielrechnung der EU-Studie 2001 (siehe Seite 41) belegt dies bereits für ein einfaches opt-out, zudem stellt aus europäischer Perspektive jede spam mail bereits eine Verletzung der Grundrechte natürlicher Personen dar. Die Teilnahme an einem einfachen opt-out-Verfahren erfordert jedoch mindestens eine spam mail. Einer Email-Adresse ist nicht der geographische Standort ihres Inhabers zu entnehmen. Eine Email-Adresse ist aber stets an einen Server gebunden. Das global opt-out-Verfahren der USA müsste daher ein allgemeines opt-out ganzer Server ermöglichen, dann könnten alle europäischen Server und die durch sie bedienten Email-Adressen bis zu einem gegenteiligen opt-in vom spam-Versand ausgenommen werden. Das opt-out ganzer Server umgeht auch das Problem, Listen europäischer Email-Adressen, personenbezogener Daten, in die USA exportieren zu müssen.[31] Eine entsprechende Gestaltung des Codes (im Sinne von Lawrence Lessig, [Lessig 1999]) ließe eine Vermittlung zwischen den Interessen von EU und USA zu.

Es ist denkbar, dass ein global opt-out ganzer Server bzw. ausländischer Server nicht zulässig ist, da es als Eingriff in die Redefreiheit gewertet wird. Denkbar ist aber auch, dass das US-Recht europäischen Nutzern einen anderen Schutz gewährt als

31 Für einen entsprechenden Export gilt im Übrigen das safe harbour-Abkommen.

amerikanischen. Dies wäre nicht das erste Mal. 2001 vereinbarten die USA und die EU das safe harbour-Abkommen.[32] Dies gewährt den personenbezogenen Daten von EU-Bürgern in den USA einen höheren Schutz als den Daten von US-Bürgern. Das Abkommen verdankt seinen Namen dem in der EU-Datenschutzrichtlinie (1995/46/EG) niedergelegten Prinzip, das personenbezogene Daten nach EU-Recht und entsprechender Umsetzung der Mitgliedsstaaten nur in Staaten mit gleichem, angemessenen Datenschutzniveau exportiert werden dürfen, wenn das Exportland ein sicherer Hafen ist. Bildet das Exportland keinen sicheren Hafen, so muss der Exporteur dafür sorgen, dass die Sicherheit der Daten auf anderem Wege – in der Regel durch Vertrag – gewährleistet ist oder darf die Daten nicht exportieren. Um den Export personenbezogener Daten in die nicht als sicherer Hafen geltende USA zu erleichtern, haben die USA und EU das safe harbour-Abkommen geschlossen. Es sieht vor, dass US-Unternehmen dennoch als sicherer Hafen gelten, wenn sie gegenüber dem US-Handelsministerium erklären, dass sie die Regeln des EU-Datenschutzes befolgen. Der Schutz personenbezogener Daten erstreckt sich dann auch auf die Daten von US-Bürgern. Eine Verletzung des zugesagten Datenschutzniveaus gilt in den USA als Verstoß gegen das Wettbewerbsrecht (unlauterer Wettbewerb) und kann durch Mitbewerber und Kunden vor der FTC geahndet werden. Das amerikanische Wettbewerbsrecht schützt ein europäisches Grundrecht.

Die Vereinbarkeit einer europäischen opt-in-Lösung und einer amerikanischen opt-out-Lösung ist an Voraussetzungen bei der Implementation gebunden. Implementation bezieht sich hier auf die Umsetzung einer Politik, ihre juristische Kodifizierung und auch die technische Realisierung. Rechtliche Voraussetzungen sind die Beteiligung und die Art der Beteiligung europäischer Nutzer. Technische Voraussetzungen ist ein Registrierungsmechanismus, der die Aufnahme ganzer Server und / oder europäischer Email-Adressen in diese Robinson-Liste für spam ermöglicht.

Voraussetzung für die Kooperation ist, dass beide Akteure – USA und EU – ein Interesse an ihr haben. Nachfolgend wird in Anlehnung an die Spieltheorie[33] eine Auszahlungsmatrix entwickelt, die darlegt, wie die Gewinnverteilung ist, wenn beide hier kooperieren.

Beide Akteure haben entsprechend Gesetze erlassen, die für Werbe-Emails einen remove request vorschreiben. Interessensgleichheit ist hier gegeben. Remove requests sind in Werbe-Emails (permission based marketing) und spam aus den USA zu

32 Information zum Verfahren finden sich unter http://www.export.gov/safeharbor/
33 Zur Spieltheorie siehe zum Beispiel [Scharpf 2000], S. 24ff

erwarten. In den USA treffen ausschließlich Werbe-Emails aus der EU ein, die der Empfänger angefordert hat und die zwingend einen remove request enthalten. Die Grundrechte und somit der Datenschutz gelten innerhalb der EU auch für US-Bürger. Das spam-Problem stellt sich allein als ein us-amerikanisches dar. Europäischer spam ist auch vom Volumen her unproblematisch. Berichten einiger ISPs zufolge beträgt der Anteil aus den USA importierten spams 80% (siehe [EU-Studie 2001], S.89)

Ein Blick[34] auf die von Spamhaus geführte ROKSO-Liste zeigt, dass von 179 gelisteten spammern der Großteil aus USA stammt – 135 bzw. 79,4%. Nur sechs (3,5%) sind in EU-Ländern ansässig[35]; auf übrige Länder entfallen 29 (17,1%).[36] Eine erfolgreiche Bekämpfung von spam in europäischer Perspektive würde bedeuten, dass europäische Nutzer weitgehend von amerikanischen spam befreit werden.

Vielfach wird gegen das Funktionieren derartiger Lösungen ins Feld geführt, dass es für spammer einfach sei, das Land zu wechseln. Eine Betrachtung des spam-Problems außerhalb der USA und der EU fand bisher nicht statt. Der große Anteil amerikanischer spammer auf der ROKSO-Liste zeigt, dass die Bekämpfung von spam auch in den USA erfolgen muss. Von dort kommt auch der meiste spam, der europäischen Nutzern zugeht. Die Zahl der spammer ist rückläufig, weltweit sind es gerade 200 bis 250 spammer, die für 90% des spams verantwortlich sind. (vgl. [Spamhaus] zu Zahlen, [EU-Studie 2001] zum Trend) Ein Rückgang der Zahl der spammer ist bisher aber nicht mit einer Reduzierung des spam-Volumens einhergegangen. Ohne Gegenmaßnahmen wird sogar befürchtet, dass das Volumen weiter zunehmen wird (vgl. z.B. [Delio 2003d]). Die geringe Zahl an spammer zeigt auch, dass aufgrund rechtlicher und technischer Gegenmaßnahmen spamming kein einfaches Geschäft mehr ist und dass es Spezialkenntnise erfordert.

Die antispam-Organisation CAUCE weist darauf hin [CAUCE 2004], dass ein Ausweichen der spammer ins Ausland nicht viel bringen würde. Spam bietet in der Regel Waren an, die innerhalb der USA bestellt, versandt und per Kreditkarte bezahlt werden. Europäische Nutzer können regelmäßig mit den angebotenen Waren und Dienstleistungen wenig(er) anfangen, da sie sie nicht bestellen können oder eine Lieferung aus den USA sehr teuer ist. Bei den mit spam Beworbenen handelt es sich überwiegend um US-Unternehmen, die die eigentlichen Verursacher sind, selbst wenn der Versand aus dem Ausland erfolgt. Wenn als Verstoß gegen den CAN SPAM act

34 Daten vom 20. Februar 2004, 12.15 Uhr MEZ
35 Lettland wurde bei der Auswertung zu den EU-Länder gezählt; zur Definition von spam siehe [Spamhaus] und Seite 33
36 Kanada 10, Australien 6, Argentinien 3, Russland 3, Costa Rica 2, China 1, Indien 1, Philippinen 1, Taiwan 1, Hongkong 1

eine physische Adresse nicht angegeben ist, so bleibt stets die Möglichkeit der Spur des Geldes zu folgen. Paul Graham, bekannter antispam-Aktivist und Erfinder der derzeit weit verbreiteten Bayes'schen Filter, fordert neuerdings sogar den Rückgriff auf beteiligte Kreditkartenunternehmen [Dean 2004]. Wie bereits dargelegt folgt spam ökonomischer Prinzipien, so dass die Unterbrechung des Geldflusses hilfreich erscheint. Andere Ansätze verfolgen eine Gewinnabschöpfung bei spammern und den mit spam Beworbenen.

Die Bekämpfung des spam aus den USA lohnt, weil der Großteil des spams von dort stammt und ein Ausweichen der spammer in andere Länder ökonomisch wenig sinnvoll ist. Deutlich weniger spam wird innerhalb der EU versendet.

Zwei Gründe haben dazu geführt, dass ein europäisches spam-Problem nicht entstanden ist: Zum einen kommt dem Datenschutz ein höherer Stellenwert zu, zum anderen wurde das spam-Problem bereits diskutiert, als es noch gar nicht existierte (vgl. [EU-Studie 2001], S.89). Aus europäischer Sicht ist spam weitgehend ein Importprodukt. Nicht alle Europäer haben Englisch als Muttersprache. Die Sprachbarriere verstärkt dies noch, da spam für Sprachen mit wenigen Millionen sprechenden deutlich weniger attraktiv ist. Zur Bekämpfung von spam aus europäischer Perspektive ist die Kooperation der USA unbedingt erforderlich. Für die USA ist auf den ersten Blick eine Kooperation der EU nicht zwingend erforderlich. Europäische Werbe-Emails des permission based marketing genügen der amerikanischen Forderung eines remove requests; bezüglich der physischen Adresse ist dies nicht immer der Fall. Ein opt-out ist somit auch für US-Nutzer möglich.

Die EU scheint von einseitigem Handel der USA abhängig zu sein, die selbst kein Interesse an der Änderung der Politik der EU haben. Bei einer derartigen einseitigen Abhängigkeit empfiehlt sich eine Verquickung mit anderen Problemen oder sogar Politikfeldern, um gegebenenfalls ein bargaining zu ermöglichen. Denkbar wäre auch eine Sanktionierung aller amerikanischen Versender von Emails, was jedoch als Strategie unwahrscheinlich ist, da auch die EU an einem funktionierenden Email-System interessiert ist. Eine Hürde, die zum safe harbour-Abkommen führte, waren Exporterschwernisse für personenbezogene Daten infolge der EU-Richtlinie 1995/46/EG. Derartige Erschwernisse sind kaum im Interesse der USA, so dass die USA auch an kooperativem Verhalten interessiert sind, um sie zu vermeiden.

Die Reduzierung des Aufkommens an spam und der damit verbundenen Kosten ist auch im Interesse der Dienstleister, die die Infrastruktur des Internets – Leitungen, Server, etc. – bereitstellen. Diese Internet Service Provider(ISP) sind großteils in den

USA ansässig und unterstützen politische und technische Maßnahmen zur spam-Bekämpfung.

Ohne Kooperation der USA bliebe der EU nur zu hoffen, dass die erfolgreiche Implementation des global opt-ou-Verfahrens, die Ökonomie - wie vorher geschildert – verändert. Dies ist aber hoch spekulativ und bereits an den Erfolg des global opt-out-System gebunden.

### *Übermittlung*

Einer Studie von Ferris Research [Ferris 2003b] nach verursacht spam in 2003 allein für die ISPs Kosten in Höhe von US-$ 500 Mio. Der Overhead an Transfervolumen für Datenpakete, die durch spam verursacht werden beträgt 10%; allerdings ist die Definition von spam hier unklar.
Wie eingangs dargelegt entstehen auch bei US-Firmen Kosten durch spam in geschätzter Höhe von 10 Milliarden US-$ in 2003 (zum Vergleich Verlust für EU-Firmen in 2002 geschätzte 2,5 Milliarden Euro) (Zahlen: [Wired News 2003c], [Ferris 2003]) Ebenso wie Firmen versuchen ISPs durch den Einsatz von Technik und Personal die spam-Flut zu bekämpfen. Die ISPs sowie die Anbieter entsprechender anti-spam-Software (anti-spamware) konkurrieren untereinander, wie zum Beispiel AOL, Yahoo! und GMX. Computerzeitschriften mit Testberichten zum ISPs und anti-spamware komplettieren den Markt, für den ein weiteres Wachstum vorausgesagt ist - von US-$ 653 Mio. in 2003 zu US-$ 2,4 Mrd. in 2007 (siehe [Asaravala 2003b]).

US-Firmen, die auf ein vollständiges opt-out ihrer Server drängen, wollen nicht nur ihre Mitarbeiter davon befreien, sondern auch ihre Netze von Irrläufern und error traffic. Mit der EU teilen sie das Interesse, am globalen opt-out-System der FTC ganze Server anmelden zu können. Sogar ein opt-out sämtlicher europäischer Server ist im Interesse der großen us-amerikanischen und multinationalen ISPs.

Das Internet entstand historisch aus dem Verbund mehrerer regionaler Netze. Die Topographie des Internets erfordert einen globalen backbone, ein Netz an leistungsfähigen Interkontinentalverbindungen. Die Interlinks zwischen beiden Ufern des Atlantiks werden von wenigen großen ISPs betrieben und laufen durch wenige wichtige Austauschpunkte für TCP/IP-Datenpakte, zum Beispiel MAE East und MAE West; [AP 2003g] berichtet, dass 50% des weltweiten Datenverkehrs durch den US-Bundesstaat Virginia läuft. Die Topographie des Netzes verstärkt um einige Besonderheiten der europäischen Netztopographie bewirkt, dass der Großteil der in Europa eintreffenden spams die Leitungen dieser ISPs stark belastet.

Eine der größten Anbieter u.a. an Email-Dienstleistungen ist AOL, das seit Januar 2004 das SPF-Protokoll als open-source-Software freigegeben hat und propagiert, um den Ursprungsserver eindeutig identifizieren zu können. Mit einer Änderung des Codes des Internets versucht AOL, spam zu bekämpfen.

Zwar sind US-Verbrauchorganisationen nicht direkt an einer Reduzierung des in Europa eintreffenden spams interessiert, aber ein server-weites opt-out deckt sich mit ihrem Interesse, spam für die US-Nutzer zu reduzieren. Bei IPSs, US-Verbraucherorganisationen besteht weitgehend Interessensgleichheit. Diesen Interessen stehen die Ziele einiger Marketingverbände entgegen, zum Beispiel der DMA (siehe Seite 43), die ein opt-out ganzer Server bei dem von ihr in Eigenregie betriebenen Do-Not-E-Mail-System ablehnt.

EU und USA teilen das Ziel, das Internet – e-business und e-government – zu fördern. Email als Killerapplikation des Internets kommt eine Schlüsselrolle zu. Nur ein ungestört funktionierender Email-Dienst gewährleistet eine hinreichende Akzeptanz durch die Nutzer. Eine Ausweitung der Nutzung in Europa liegt auch im Interesse der USA. Nicht zuletzt vergrößern sich hierdurch für US-Unternehmen die Märkte.

Vor dem Hintergrund unterschiedlicher Präferenzen, die auch in den unterschiedlichen Definitionen von spam zum Ausdruck kommen ist es denkbar, dass die US-Regierung das Ziel eines weitergehenden spam-Schutzes für EU-Bürger akzeptieren kann. Vergleichend kann hier das safe harbour-Abkommen betrachtet werden, das EU-Bürgern ein höheres Datenschutzniveau in den USA gewährleistet. Entsprechende rechtliche Konstrukte wären zu entwickeln.

In Hinsicht auf die im first amendement der US-Verfassung verankerten Redefreiheit ist auch zu berücksichtigen, ob eine entsprechende weitergehende Beschränkung des Versands von spam durch US-Bürger an EU-Bürger als unzulässigen Eingriff gelten kann. Da sich ein Großteil des spams nur an US-Bürger richtet, genügt wahrscheinlich schon die optionale Bereitstellung eines globalen opt-outs aller europäischen Server im Rahmen des geplanten opt-out-Verfahrens der FTC.

Tabelle 8 zeigt die Auszahlungsmatrix, die die Gewinne bei einer kooperativen Lösung darstellt. Kooperativ bedeutet bezüglich der USA, dass diese weitgehend die Interessen der EU berücksichtigen. Kooperativ bedeutet bezüglich der EU, dass diese auf Sanktionen verzichtet und auf die Implementation Einfluß nimmt.

| | | | **USA** | |
|---|---|---|---|---|
| | | | Kooperativ | Nicht-kooperativ |
| **EU** | Kooperativ | EU | 3 | 0 |
| | | USA | 3 | 1 |
| | Nicht-kooperativ | EU | 2 | 0 |
| | | USA | 2 | 1 |

*Tabelle 8 Auszahlungsmatrix*

Folgende Punkte wurden in dieser Auszahlungsmatrix vergeben:

- Bei Umsetzung ihrer jeweiligen Vorstellung hinsichtlich ihrer Perspektive auf spam erhalten die EU und die USA je einen Punkt.
  Aus der EU stammende Werbemails sollen einen remove request enthalten. Spamming ist hier deutlich seltener als in den USA. Dem opt-out-Schema ist genüge getan, auch wenn die im CAN SPAM act vorgesehene physische Adresse nicht unbedingt in einer europäischen Werbe-Email enthalten sein muss.
  All dies gilt auch für legitime Werbe-Emails amerikanischen Ursprungs. Da die EU jedoch ein opt-in-Verfahren vorschreibt, genügen amerikanische Emails regelmäßig nicht den höheren europäischen Maßstäben. Eine einseitige Politik der USA hilft der EU nicht weiter.

- Ein weiterer Punkt wird vergeben, falls die Teilnahme am geplanten global opt-out-Verfahren der FTC sowohl amerikanischen, als auch europäischen Nutzern möglich ist. Wie dargelegt reduziert dies die Kosten der ISPs, was auch im Interesse der US-Regierung liegen sollte, und bietet den EU-Nutzern die Teilnahme am amerikanischen global opt-out, selbst wenn dies nicht äquivalent zu einem opt-in-Modell ist. Eine Partizipation der EU-Nutzer kann auch einseitig durch die USA ermöglicht werden.

- Ein globales opt-out aller europäischen Email-Adressen oder zumindest der hier ansässigen Server können die USA auch durch einseitiges Handeln einrichten. Eine Kooperation mit der EU ist nicht nötig. Auf juristische und ggf. politische Probleme hinsichtlich eventueller Einschränkungen der Redefreiheit wurde bereits eingegangen. Als unwahrscheinlich wird erachtet, dass die US-Regierung ohne weitere Beweggründe die weitergehenden Interessen der EU bezüglich spam berücksichtigt. Erst die Einflussnahme von EU und ISP zusammen mit einem generellen Interesse an der weiteren Verbreitung des Mediums Internet dürften ausschlaggebend sein. Verfassungsrechtliche Probleme seinen zunächst hinten angestellt. Ein optionales Angebot im Rahmen

des geplanten opt-out-Systems der FTC kann, wie bereits gesagt, ausreichend sein. Insgesamt lohnt sich für die USA kooperatives Verhalten wie auch für die EU; für letztere sogar noch stärker, da die EU nur so ihr opt-in-Modell für ihre Nutzer weitgehend durchsetzen kann.

Eine Koexistenz eines opt-in-Verfahrens und eines globalen opt-out-Schemas im Cyberspace ist möglich, sofern das opt-out-Verfahren alle Nutzer des opt-in-Verfahrens berücksichtigt. Diese Berücksichtigung liegt im Interesse beider Akteure, der USA und der EU. Voraussetzung für diese Koexistenz ist die erfolgreiche technische und gesellschaftliche Implementation des global-opt-out-Verfahrens der FTC.

Ein Blick auf die Auszahlungsmatrix zeigt zudem, dass kooperatives Verhalten den USA keinen Nachteil bietet. Ein Gewinn lässt sich unabhängig vom Verhalten der EU immer realisieren. Für die EU ist kooperatives Verhalten der USA zwingend erforderlich, da es Voraussetzung für jeglichen Gewinn ihrerseits ist.

An dieser Stelle sei eine Prognose gewagt. Mit dem Aufbau des global opt-out-Verfahrens durch die FTC wird gemäß des im CAN SPAM act verankerten Zeitplans nicht vor Herbst 2004 zu rechnen sein. Bis dieses Verfahren technisch realisiert und eine hinreichende Partizipation der Nutzer gegeben ist, dürfte ein weiteres Jahr vergehen. Der Erfolg hängt auch von einer entsprechenden gesellschaftlichen Akzeptanz des Verfahrens und gegebenenfalls staatlicher Sanktionen bei Nichtbeachtung ab. Für diese Stufe der Implementation veranschlage ich ein weiteres Jahr. Da das Funktionieren des global opt-out-Schemas Voraussetzung für ein effektives opt-in-Schema innerhalb der EU ist zwingend erforderlich ist, sind so entsprechende Vereinbarungen zwischen EU und USA über eine Partizipation der EU am global opt-out-Verfahren der USA nicht vor 2007 zu erwarten. Frühestens 2008 ist dann ein Lösung des spam-Problems aus europäischer Perspektive zu erwarten. Einseitiges Handeln der USA und politischer Wille den Verhandlungsprozess frühzeitig aufzunehmen und zu beschleunigen, könnten ihn verkürzen.

Nachfolgend einige Argumente, die unterstützen, dass kooperatives Verhalten seitens beider Akteure als sinnvoll erachtet wird und diese daher zu Verhandlungen bereit sind:

- Im CAN SPAM act formuliert der US-Kongress im Abschnitt "CONGRESSIONAL FINDINGS AND POLICY" den Zwang zur Kooperation mit anderen Staaten, die nötig ist, um das spam-Problem zu lösen: *"The problems associated with the rapid growth and abuse of unsolicited*

*commercial electronic mail cannot be solved by Federal legislation alone. The development and adoption of technological approaches and the pursuit of cooperative efforts with other countries will be necessary as well."* (CAN SPAM act of 2003, section 2 a) (12))

- Über den CAN SPAM act wird beklagt, dass er das Klagerecht bei Verstößen bei der FTC konzentriert. Ein Klagerecht Privater ist nicht gegeben. Es wird bemängelt, dass die eine effektive Durchsetzung des CAN SPAM acts verhindere.
  Die derzeitige Begrenzung der Klagerechte erleichtert der US-Regierung Verhandlungen darüber, wie er bei Berücksichtigung ausländischer Interessen zu gestalten wäre. Beim safe harbour-Abkommen war bemängelt worden, dass Verstöße zwar vor der FTC verfolgt werden können, dies für EU-Bürger aber mit einem immensen Aufwand verbunden ist. Ein bereits für Private eröffneter Klageweg könnte die US-Regierung zur Berücksichtigung von Interessen zwingen, die Verhandlungen erschwerten.

- Um Verhandlungen zu erleichtern ist idealiter klar, worüber verhandelt wird und welche Ziele die Akteure verfolgen. Der CAN SPAM act trat zum 1. Januar 2004 in Kraft, die EU-Richtlinie 2002/58/EG forderte von den Mitgliedsstaaten die Umsetzung in nationales Recht bis Ende Oktober 2003.
  CAN SPAM act und EU-Richtlinie geben den Verhandlungsführern quasi ein Mandat und Klarheit darüber, was sie zu vertreten und zu erreichen haben.

- Im Rahmen der OECD finden erste Beratungen hierüber statt. Erste Vereinbarungen der OECD wurden im Juni 2003 getroffen [NZZ Online 2003].
  Anfang Februar 2004 fand eine erste Konferenz der OECD zu spam in Brüssel statt [Ermert 2004]. Die OECD als Vereinigung westlicher Industrienationen, die auch das Internet dominieren, ein Forum dar, das mit seinen Strukturen geeignet ist, nicht nur eine Verhandlungslösung zwischen den EU und USA, sondern zwischen den durch sie vertretenenen Gruppen von Ländern mit einer opt-in- bzw. opt-out-Lösung. Dem Begleitpapier zur OECD-Konferenz zu spam Anfang Februar ist eine Übersicht der Mitgliedsländer zu entnehmen, die eine opt-in- bzw. opt-out-Lösung haben oder anstreben; der Übersicht ist auch zu entnehmen, dass die EU-Richtlinie 2002/58/EG zu ein Änderung der Politik einiger EU-Länder, z.B. der Niederlande, geführt hat. Weitere Vertreter eines opt-out-Modells sind einige ostasiatische Länder.

### *Empfang*

Nicht jede spam mail, die versandt wird, wird auch empfangen. Spam mails an nicht-existierende bzw. nicht mehr existierende Email-Adressen erhöhen das Transfervolumen und erzeugen zu dem error traffic. Mit diesem Problem haben nicht nur die ISPs zu kämpfen, sondern auch spammer, denen Beschwerden über spam und error traffic zugestellt werden. Eine Lösung war bisher, dass falsche Absenderangaben benutzt wurden. Die Folge ist, dass der error traffic durch weiteren error traffic weiter das Transfervolumen erhöht, bis die Endlosschleife durchbrochen wird, oder der error traffic an Email-Adressen geht, deren Inhaber durch die Flut an für sie sinnlosen Emails geschädigt werden. (siehe z.B. [Delio 2003e]) Die Schädigungen reichen bis zum Ruin von Firmen.
Der CAN SPAM act stellt bereits das Vertuschen von oder Täuschung über Absenderangaben unter Strafe. Email-Adressen-Verzeichnisse, die zufällig oder systematisch Email-Adressen erzeugen, stellen hier ein besonderes Problem. Programme – spamware –, die derartiges ermöglichen, sind dem CAN SPAM act nach nun verboten. In der EU ist derartige Software nicht einheitlich verboten, allerdings ist das Anlegen entsprechender Datenbanken aufgrund des allgemeinen Datenschutzes bereits eingeschränkt.

Der für Werbemails vorgeschriebene remove request gibt eine Grundlage, die Absender zu ermitteln. Ist eine physische Adresse für die EU nicht zwingend, so doch ein funktionierendes opt-out für legitime Werbe-Emails. Der CAN SPAM act schreibt vor, dass der remove request 30 Tage nach Absendung einer Email noch funktionieren muss. Der remove request erleichtert technisch das Filtern von spam, aber auch die Ermittlung der Absender. Übriger spam gilt per se bereits als illegal, da er die für die Rückverfolgung nötigen Daten nicht enthält. Das Fehlen dieser Angaben rechtfertigt bereits eine Sanktionierung. Insbesondere betrügerischer spam wird so hoffentlich unterbunden werden können, da dieser seiner Art nach fälschliche Angaben über die wahren Initiatoren benötigt. (Vgl. Berichterstattung über den Nigeria Scam: [Wired News 2003b] und [Roth 2004])

Aus der Beispielrechnung der EU-Studie (siehe Seite 41) bzgl. Opt-out-Verfahren und entsprechend meiner Schätzung, bis wann mit einer Lösung des spam-Problems zu rechnen ist,  ist zu folgern, dass in den nächsten Jahren weiterhin ein spam-Problem existieren wird. EU-Nutzer werden zunächst nicht von amerikanischem spam verschont, US-Nutzer werden auch gegen spam mit remove request verschont bleiben wollen, solange das global opt-out-Verfahren noch nicht hinreichend funktioniert.

Dies garantiert weiterhin einen – sogar wachsenden – Markt für antispam-Software, allen voran von Filtersoftware für Endnutzer und ISPs.
Erst das Funktionieren des global opt-out-Schemas und eine Berücksichtigung europäischer Interessen dürfte eine Trendwende für diesen Markt bedeuten. Da nicht mit einem vollständigen weltweiten Verschwinden von spam in allen Formen zu rechnen ist, wird weiterhin ein - wenn auch geringerer - Bedarf an dieser Software bestehen.

Durch Verhandlungen zur Vereinbarkeit von opt-out- und opt-in-Schema wird versucht, bereits das Einspeisen von spam zu bekämpfen. Sollten diese Verhandlungen scheitern, dann stellt die Filterung von spam – zumindest für Länder mit opt-in-Modell und Nutzer, die mit dem opt-out-Verfahren nicht zufrieden sind – eine allerdings problembehaftete Lösung zur Reduzierung der spam-Flut dar. Filtersoftware und Anbieter entsprechender Dienstleistungen konkurrieren hier. Ein Eingriff des Staates zugunstenvon antispam-Software ist denkbar, wenn die Verhandlungen bzgl. einer Begrenzung von spam an der Quelle scheitern. Die Stärkung formeller Kriterien, wie im CAN SPAM act und in der EU-Richtlinie 2002/58/EG ist ein erster Schritt hierzu. Beide verbieten falsche Angaben zum Absender.

## 3. Nebeneffekte

Ziel der Politik ist derzeit, eine Lösung für spam zu finden, die bereits seine Entstehung, sein Einbringen ins Internet verhindert. Diametral entgegengesetzt sieht hier die Wahrnehmung für den Nutzer, den Bürger, aus. Dieser kämpft am Ende der Kette mit der spam-Flut. Er hofft auf die Wirksamkeit von antispam-Software, die käuflich erworben werden und deren Behandlung derzeit viel Platz in Computerzeitschriften einnimmt. „*Going Upstream to Fight Spam"* [Baard 2004] ist der politisch-rechtlich viel versprechendste Ansatz. Die rechtliche Behandlung des Themas spam wird dabei inzwischen als Schlüssel zu einer Lösung betrachtet („key tool" - [OECD 2004], S.23). Zudem wird hier ein Regulierungsbedarf durch den Staat – in Kooperation mit anderen Staaten – gesehen. So bedeutete der Erlass des CAN SPAM acts eine Ausnahme – ggf. sogar eine Umkehr – einer us-amerikanischen Politik unter Georg W. Bush und bereits seinem Vorgänger Bill Clinton, die (auch) das Internet möglichst nicht regulieren will. (siehe Berichterstattung [AP 2003e])

Am weitestgehenden ist der Ansatz, bereits das Sammeln von Adressen zu beschränken. Aufgrund eines in den USA fehlenden allgemeinen Datenschutzrechts behilft sich der Kongress mit einem Verbot von spamware, die die Adresssammlung automatisiert. Die Aufnahme von Adressen in derartige Sammlungen – manuell oder automatisiert – ist nach der allgemeinen Datenschutz-Richtlinie der EU (1995/46/EG) bereits unzulässig; für ein Verbot entsprechender Software, die meist auch zu legitimen Zweck verwendet werden kann, bestand hier kein Bedarf.

Im vorherigen Abschnitt wurde dargelegt, dass EU und USA Interesse an einer kooperativen Lösung haben. Sollten die Verhandlungen so verlaufen, so dass kein Erfolg erzielt werden kann, dann werden andere Lösungen an Bedeutung gewinnen. Diese Lösungen bringen andere Probleme, die als Nebeneffekte auftauchen, von einigen Akteuren der politischen System aber durchaus bevorzugt werden könnten.

Da alle Regulierungsinstrumente in ihren Leistungen begrenzt sind, spricht vieles für einen multi-dimensionalen Ansatz („multi-dimensional apporach", [OECD 2004], S.31). Das Scheitern einer Verhandlungslösung, wie vorher dargelegt wurde, würde für das Ziel der erfolgreichen spam-Bekämpfung bedeuten, dass die übrigen Lösungsansätze samt ggf. negativ erachteter Nebeneffekte verstärkt werden müssten, ja staatlicher Unterstützung bedürften. Alternativ könnte das Ziel der spam-Bekämpfung fallengelassen werden. Die Nebeneffekte werden hier auch angeführt, um den Sinn und die Eleganz einer kooperativen Lösung zur Vereinbarkeit von opt-in- und opt-out-Verfahren aufzuzeigen.

> »As usual, we discuss solutions drawn from technology, market pressure, business policies and law.« [Baase 2003] (S.220)

Vier Regulierungsinstrumente sind gesellschaftliche Normen, Gesetze, Marktmechanismen und Architektur. Bezüglich des Internets wird letztes hier mit Lawrence Lessig [Lessig 1999] als Code bezeichnet, was Sara Baase Technologie nennt.[37]

Gesetzliche Regelungen sind Lösungen, wie sie im vorherigen Abschnitt geschildert wurden. Da das Internet in seiner derzeitigen Form keine Grenzen hat, muss eine weltweit einheitliche Lösung angestrebt werden.[38] Teilerfolge würden ggf. Grenzen im Internet errichten, wobei fraglich ist, ob dies überhaupt möglich ist. Dieser Errichtung von Grenzen wäre nur mit einem massiven Eingriff in den Code des Internets zu erreichen. Dieser Eingriff in einheitlicher Gestalt ist nur durch eine indirekte Regulierung durch den Staat bzw. die Staaten denkbar. Sie könnten per Gesetz dem Code seine Struktur vorschreiben (vgl. [Lessig 1999], S.164ff – insb. S.170). Diese Fähigkeit des Staates zur indirekten Regulierung des Codes wird jedoch stark eingeschränkt durch open-source-Software, die gerade Grundlage von Protokollen und Software des Internets sind [Lessig 1999] (S.181); dies bedeutet auch, dass dieser geschwächte Staat mehr auf Lösungen mit anderen Regulierungsinstrumenten setzen muss, zum Beispiel die Lösung des vorherigen Abschnitts. Denkbar ist auch, dass dieser Staat dann von einer Lösung am Beginn von spam absieht und den Einsatz bestimmter Software, zum Beispiel Filtersoftware, an bestimmten Stellen im Netz, zumindest für sein Hoheitsgebiet, vorschreibt.

Dieser Staat kann aber auch Normen beeinflussen. Bezüglich des geringeren spam-Problems in Europa wird immer wieder auf den höheren Stellenwert des Datenschutzes verwiesen. [Fallows 2003] zeigte auch, dass Jüngere besser mit spam fertig werden als Ältere (s. S.12). Über Normen kann auch das Nutzerverhalten verändert werden. Im Internet, Computerzeitschriften und Büchern finden sich zahlreiche Ratschläge, wie der Nutzer verhindern kann, dass seine Adresse in die Sammlungen von Spammern aufgenommen wird und wie er mit eintreffendem spam fertig wird. Auch die FTC hat einen derartigen Ratgeber herausgegeben [FTC 2002] und betreibt eine Kampagne, Server-Betreiber dazu zu bewegen, Sicherheitslöcher, die spammer nutzen, zu schließen.[39]

37 Bei [Baase 2003] handelt es sich um ein aktuelles, amerikanisches Standardwerk zu sozialen, ethnischen und rechtlichen Fragen des Internet, bei der viel zu kurzen Analyse zu spam, bleibt es hinter den Erwartung zurück.

38 nach [Lessig 1999] ist der „Cyberspace nicht ein Ort, sondern viele“ (S.121), allerdings kennt dessen Architektur -der Code- derzeit keine Grenzen.

39 siehe „Operation Secure Your Server“ mit diversen Broschüren (PDF): http://www.ftc.gov/secureyourserver

Marktmechanismen scheinen bisher nicht verwendet zu werden, um spam zu bekämpfen. Allenfalls können Marktmechanismen hinsichtlich spam in zwei Formen entdeckt werden: Zum einen sind dort die Lösungsansätze zu nennen, die die Ökonomie des spams verhindern. Diese erfordern stets einen Eingriff in den spam, wenn es sich nicht ausschließlich um Sanktionen wie Strafen und Gewinnabschöpfung handelt. Zum anderen findet unter den Providern von Email-Diensten auch eine Konkurrenz um Kunden über die Effektivität der eingesetzten Filter statt.
Email steht natürlich auch in Konkurrenz zu anderen Medien, aber eine Flucht aus dem Medium ist noch nicht zu erkennen, auch wenn Tomas Janot plakativ ruft: *"Wegen des Spams lese ich eh keine Mails mehr."* (siehe Seite 26).

## *Änderung der Funktionsweise des Internets*

Lösungen für das spam-Problem sehen Änderungen an der Funktionsweise des Email-Dienstes vor, die auch die Ökonomie von spam entscheidend verändern. Zwei ausgewählte Lösungsansätze seien hier dargestellt.

### Elektronische Briefmarken

Selbst bei geringen Kosten von einem Tausendstel Cent pro Email würde sich der massenhafte Versand nicht mehr lohnen, so lautet die These. Eine Million spam würden dann zumindest 1000 Dollar oder Euro kosten, die zunächst einmal erwirtschaftet werden müssen. Wird bei herkömmlichem Direktmarkting von einer Rückmeldequote von unter einem Prozent ausgegangen, dann müssten sich mit weniger als 1000 Kundenkontakten bei einer Million verschickten spam mails pro Kontakt mehr als 1 Euro bzw. Dollar erwirtschaften lassen. Die Quote liegt derzeit bei weniger als 15 Kontakten je eine Million spam; pro Kontakt wären dann mehr als 66 Dollar bzw. Euro, die erwirtschaftet werden müssten. Bei den wenigsten per spam angebotenen Produkten dürfte dies möglich sein. (vgl. FTC-Liste, Seite 17)

Problematisch ist bei diesem Lösungsansatz, dass eine Infrastruktur zur Zahlungsabwicklung aufgebaut werden muss. Diese Infrastruktur könnte Anonymität verhindern, da Zahlungsvorgängen gefolgt werden könnte. Außerdem ist vorstellbar, dass spam weiter erhalten bleibt, allerdings Firmen, die die Kontrolle über die Infrastruktur haben, dafür bezahlt werden müssten. Dies dürfte aber zumindest zu einer Reduzierung des spam führen.

#### Rechenzeit als Briefmarke

Einen ähnlichen Ansatz wie die elektronische Briefmarke für Emails verfolgen Lösungen, die mit Rechenzeit bezahlen. Hier muss von einem Client eine komplexe Re-

chenaufgabe gelöst werden, bevor ein Server eine Email zum Versand annimmt. Diese Rechenaufgabe muss so komplex sein, dass sie hinreichend Rechenzeit verbraucht, um den massenhaften Versand von Emails zu verhindern. Würde der Versand eine Rechenzeit in Höhe von einem Zehntel einer Sekunde – was der Nutzer kaum merken würde -, so würde der Versand einer Million spam bereits Rechenzeit von mehr als 27 Stunden erfordern. Weitere Fortschritte bei der Chiptechnologie lassen jedoch befürchten, dass die benötigte Zeit im Laufe weniger Jahren schrumpfen würde.

Wie beim Ansatz elektronischer Briefmarken ist problematisch, dass das System nicht umgegangen werden darf, was nur durch den Verbrauch von Rechenzeit bei jeglicher Weitergabe an einen Server zu erreichen ist, der für alle ISPs die Kosten erhöht, die bereits jetzt Millionen an regulären Emails zustellen. Nur eine vollständige Änderung des Codes zu SMTP in kompletten Internet brächte eine Lösung. Dies scheint kaum durchzusetzen, zudem sie nochmal auf den Zusammenhang von open source und staatlicher Regulierungsmacht hingewiesen. (zu den Briefmarken vgl. [Graham 2003b][40])

## Authentifizierung (trusted systems)

SMTP kennt keine gesicherte Authentifizierung des Absenders und erlaubt die Fälschung seiner Angaben und der routing information. Veränderungen des Protokolls und des Codes der SMTP-Server versprechen eine Lösung, die besseres Filtern ermöglicht und ggf. auch den erfolgreichen Zugriff auf spammer, da sie besser identifiziert werden könnten.

Lösung bestehen in einer Authentifizierung der Nutzer am SMTP-Server – bereits bei den meisten ISPs verbreitet –, als auch in der Authentifizierung der SMTP-Server untereinander. Häufig setzen spammer bisher eigene SMTP-Server auf.

Authentifizierung bedeutet das Ende der Anonymität beim Versand von Email. SPF von AOL wurde im Januar 2004 als eine Lösung veröffentlicht, eine weitere bildet die Verwendung kryptographischer Token, die ein Konsortium um VeriSign ([VeriSign 2003]) entwickelt. SPF von AOL ist ein Mittelweg, das es nur die Identifizierung des absendenden Servers garantiert, der Server-Betreiber ist weiterhin verantwortlich, was seine Nutzer machen. Sollte sich SPF durchsetzen, so ist der Ausschluss von auch mit SPF-nutzenden Servern zu erwarten, die spam versenden; das System würde dem etablierten usenet death penalty-Verfahren gleichen.
Kryptographische Token erlauben die direkte Indentifizierung eines Nutzers, nicht nur

40 In diesem Artikel gibt Paul Graham eine Übersicht und Wertung verschiedener Ansätze zur Bekämpfung von spam.

des Servers, der ihm Zugang zum Email-Dienst gewährt; kryptographische Methoden verbrauchen zudem Rechenzeit im Sinne einer Lösung nach dem Muster „Rechenzeit als Briefmarke“.

Würde zunächst die Verwendung von Authentifizierung durch einen Sender gleichbedeutend mit einem Eintrag in einer whitelist sein, so ist umgekehrt zu befürchten, dass bei hinreichender Verbreitung eines Authentifizierungssystems Emails ohne Authentifizierung – also auch anonyme Emails - nicht mehr zugestellt würden. So könnte doch noch eine Grenze zwischen zwei unterschiedlichen Email-Diensten entstehen: Ein Dienst mit spam und Anonymität, ein Dienst ohne beide. Eine eindeutige Identifizierung des Absenders würde das gerichtliche Sanktionieren von spam und das Filtern über whitelists und blacklists deutlich erleichtern

Verifizierbare Absenderangaben würden die Probleme formeller Filterkriterien in Hinsicht auf die Mehrdeutigkeit der Absenderangaben und bewussten Täuschung durch die spammer beseitigen.

### *Anonymität vs. Trusted systems*

Mit Ausnahme der Lösung „Rechenzeit als Briefmarke“ ist eindeutig, dass alle bisher geschilderten Ansätze eine Anonymität im Netz beschränken.

Wie der Konflikt zwischen Anonymität und spam ausgeht, wird nicht zuletzt vom Ergebnis einer Kooperation der USA und der EU abhängen. Zur folgenden ersten These seien zwei weitere gewagt:

- Eine Lösung des spam-Problem hat Konsequenzen für die Anonymität. Lösungen, die die Identifizierung des Absender ermöglichen, verringern zwar spam, es besteht aber die Gefahr, „dass dadurch die von weniger effizienten Architekturen ermöglichte Anonymität verschwindet.“ ([Lessig 1999], S.249 – allerdings zum Thema trusted systems und Urheberrecht) Eventuell bleibt Pseudonymität erhalten. Eine erfolgreiche Kooperation würde derartige Lösungen weniger wahrscheinlich machen.
- Veränderungen am Code des Internet., die eine stärkere Identifizierung der Nutzer zulassen, wirken sich auf andere Entwicklungen des Internets aus. Auf Basis eines trusted systems für Email – zum Beispiel mit Hilfe von Kryptographie – werden weitere Anwendungen ermöglicht, zum Beispiel die Nutzung zum Schutz von Urheber- und Verwertungsrechten.
- Umgekehrt bietet ein entsprechendes trusted system (digital right management) Möglichkeiten für einen Email-Dienst ohne spam.

Die durch den CAN SPAM act und die EU-Richtlinie 2002/58/EG erfolgte Stärkung formeller Kriterien zur Identifizierung des Absender bewirkt einen Rückgang des Grades möglicher Anonymität. Erfolge gegen die meisten spam-Arten sind aber erst zu erwarten, wenn sich diese Anforderungen auch in der Struktur des Codes niederschlagen, zum Beispiel durch die Umsetzung von SPF. Dies wird weiter den Grad möglicher Anonymität senken. Eine Kooperation von EU und USA muss aber gerade im Interesse derjenigen sein, die am Erhalt von möglichst viel Anonymität interessiert sind. Ein Scheitern würde gerade Lösungen befördern, die ein höheres Maß an Kontrolle erfordern würden, was wiederum weniger Anonymität ermöglicht

### Umgang mit false positives

Eine weitere Lösung stellt ein anderer Umgang mit den false positives. Ihr Auftreten könnte gesellschaftlich akzeptiert werden, der Umgang mit Folgen der false positives geregelt werden. Ein Akzeptieren der false positives wäre dann der Preis dafür, möglichst keinen spam mehr zu erhalten. Wie geschildert führt dies bis zur Selbstzensur und kann auch nicht akzeptiert werden, da es den Sicherheitswert der Verlässlichkeit des Email-Dienstes, einem der vier Werte der IT-Sicherheit, systematisch beeinträchtigen würde (zu IT-Sicherheit und Sicherheitswerten siehe [Winkel 2000]). Ein Dienst der nicht verlässlich arbeitet, wird kaum akzeptiert werden.

## 4. Zusammenfassung

Der erste Abschnitt zeigt, dass unerwünschte Informationen nicht nur im Email-Dienst auftreten. Die Gefahr besteht, dass diese unerwünschten Informationen die betroffenen Dienste schädigen, ihren Wert und Nutzen reduzieren. Dies würde sie für weniger Nutzer attraktiv machen.

Unerwünschte Informationen werden in den unterschiedlichen Diensten unterschiedlich bekämpft. Beim Messenger Service erfolgt einfach eine standardmäßige Abschaltung, ein Eingriff in den Code. Blog- und Suchmaschinen-spam stellen die Betreiber vor Herausforderungen, die Dienste durch Eingriffe in den Code zu schützen oder zu moderieren. Das usenet hat bereits ein wirksames System – die usenet death penalty – entwickelt. Für email spam steht eine Lösung noch aus.

Nur die Bekämpfung des email spam wird mit politischen und rechtlichen Mitteln bekämpft; höchstens der usenet spam, SMS spam und unerwünschte Telefaxe haben in der Vergangenheit ähnliches geschafft, spielen nun aber keine Rolle mehr. Die politisch-rechtliche Bekämpfung ist bedingt durch das immense Ausmaß des Problems und den Umstand, dass die Internet-Gesellschaft noch keine Lösung präsentieren konnte bzw. diese die Beteiligung aller, z.B. zur Änderung des Codes, benötigt hätte.

Eine rechtliche Lösung für spam wird von politischen Akteuren – Verbraucherverbände, ISPs, Direktmarketingvereinigungen, Politiker – derzeit bevorzugt. Sie soll bereits die Entstehung von spam verhindern.

Spam kann anhand formeller und inhaltlicher Kriterien definiert werden. Rechtliche und technische Definitionen verwenden beide Definitionen. Rechtliche Definitionen betonen die inhaltliche, technische die formelle Seite. Eine Umsetzung der Prüfung nach inhaltlichen Kriterien in Code stellt sich als schwierig dar. Die Nutzer fordern aber Lösungen insbesondere auch von den ISPs, denen nur formelle Kriterien zur Verfügung stehen.

Eine rechtliche Stärkung von formellen Kriterien beseitigt einige spam-Arten, wenn sie eingehalten oder besser durch den Code erzwungen werden:

- Rufschädigungen und Kettenbriefe, die aufgrund ihres Inhalts bereits illegal sind, können besser verfolgt werden. Die daraus resultierende abschreckende Wirkung dürfte sie weitgehend unterbinden.
- Hinsichtlich trojanischem spam dürfte eine Identifizierung diesen beseitigen, da der Urheber erkennbar wäre. Der Code müsste dies erzwingen, damit kein Versenden mit falschen Absender möglich ist, wenn ein Rechner mit einem Virus,

Wurm oder Trojaner infiziert ist. Strategien zur Umgehung der Identifizierung sind illegal, eine Änderung des Codes zur Durchsetzung der Identifizierung würde sie unterbinden.

- Bei hoaxes stellt sich dies als unwirksam dar, da der Absender aufgrund des social engineering in gutem Glauben die Email versendet. Hier hilft nur Aufklärung, allerdings ist die Menge an spam verglichen zu übrigem spam gering.

Es bleibt hinsichtlich der spam-Phänomene und email spam nur noch die Betrachtung von spam, der nicht von Vornherein betrügerisch oder schädigend ist. (Schwartz' und Garfinkels UCE und UBE):

- Massenhafter Versand als formelles Kriterium wird von den Akteuren EU und USA nicht verwendet. Es bleibt allein das Kriterium „unangefordert".
- Die Interpretation von „unangefordert" ist verschieden:
  - Die USA und sehen „unangefordert" als solange nicht berührt, bis der Empfänger Widerspruch einlegt.
  - Die EU fordert eine ausdrückliche Einwilligung, damit „unangefordert" nicht mehr gegeben ist. Allerdings begründet für sie eine bestehende Kundenbeziehung eine Ausnahme.
  - Der Unterschied zwischen den USA und der EU kommt durch eine unterschiedliche Berücksichtigung der Interessen Dritter in Abwägung zum Schutz personenbezogener Daten zustande.
    Die Berücksichtigung kommerzieller Interessen – der unternehmerischen Freiheit – führte in den USA zu einer Entscheidung zugunsten des opt-out-Verfahrens, gemildert um ein geplantes global opt-out-Verfahren. In der EU führte dieses Interesse nur zu einer Ausnahme von opt-in im Falle einer bestehenden Kundenbeziehung.[41]
  - Ein unabgestimmtes Nebeneinander von opt-in- und opt-out-Schema stellt keine Lösung für einen Email-Dienst ohne Grenzen dar, da die Empfänger, die das opt-in-Schema schützen will, noch immer von Sendern erreicht werden, für die das opt-out-Modell verpflichtend ist.
- Es mangelt an einer (technischen) Definition, die den ISPs eine einwandfreie und einheitliche Bekämpfung ermöglicht.

41 Artikel 13 Absatz 3 der EU-Richtlinie gibt den EU-Ländern die Option zur Wahl zwischen einem opt-in- und (global) opt-out-Verfahren im nicht-kommerziellen Bereich. (siehe Seite 46)

Aus folgenden Gründen besteht weiterhin ein Interesse an der Bekämpfung von spam.

- Spam verursacht Kosten bei allen Beteiligten.
- Es besteht der politische Wunsch zum weiteren Ausbau der Nutzung des Internets, zum Beispiel für e-commerce und e-government. Mehr Nutzer müssen daher erreicht werden, was durch folgende – sich ähnelnde - Gründe durch spam behindert wird:
  - Mehr Nutzer machen spam noch attraktiver. Erfolge bei der Bekämpfung von spam werden durch zusätzliche Nutzer (teilweise) kompensiert, die mit spam beschickt werden können.
  - Spam taucht aufgrund der benötigten Masse an Empfängern erst zu einem Zeitpunkt auf, zu dem das Internet sich weitere Anwendergruppen erschließt. Das Mehr an Anwendern sorgt gerade für eine Verringerung des Mehrwerts.

Eine grundsätzliche Lösung muss her, da die so eben geschilderten Mechanismen Teilerfolge kompensieren und spam so lange Kosten verursacht, solange nicht noch Emails zugestellt werden, die nach Interpretation eines Akteurs spam sind. Eine derartige Lösung müssen die USA einbeziehen, da sie weltgrößter Export von spam sind.

Die USA als weltgrößter Exporteur und Vertreter einer opt-out-Lösung und die EU als größter Block an opt-in-Befürwortern werden in diesem Konflikt stellvertretend für die Gruppen an Staaten mit opt-in- und mit opt-out- Lösungen angesehen. (siehe Übersicht der OECD in [OECD 2004])

Außer in der gegenseitigen Übernahme des anderen Verfahrens und dem Beibehalt des status quo besteht eine Lösung in einer Kooperation, die die Vereinbarkeit von opt-in- und global-opt-out-Verfahren zum Ziel hat:

> »Eine Koexistenz eines opt-in-Verfahrens und eines globalen opt-out-Schemas im Cyberspace ist möglich, sofern das opt-out-Verfahren alle Nutzer des opt-in-Verfahrens berücksichtigt. Diese Berücksichtigung liegt im Interesse beider Akteure, der USA und der EU. Voraussetzung für diese Koexistenz ist die erfolgreiche technische und gesellschaftliche Implementation des global opt-out-Verfahrens der FTC.« (siehe Seite 58)

Das Scheitern einer Kooperation birgt folgende Gefahren.

- Die EU kann nicht ohne massiven Eingriff in die Funktionsweise des Internets, den Code, ihr Problem mit insbesondere aus den USA importiertem spam lösen.
- Hierdurch ist der Nutzen des Email-Dienstes beeinträchtigt, so dass Kosten entstehen und weniger Nutzer erschlossen werden.

- Andere Lösungen für spam verringern den Grad möglicher Anonymität mehr, als dies durch eine Kooperation und durch die bisherigen Maßnahmen für eine Stärkung formeller Kriterien, wie zum Beispiel korrekter Absenderangaben, geschieht.

Hinsichtlich einer am Verhandlungstisch zu vereinbarenden Lösung kann nicht berücksichtigt werden,

- dass Innovationen der Technik das spam-Problem lösen,
- dass eine Lösung durch private Akteure schneller realisiert wird als durch politische und
- dass bereits die erfolgte Stärkung verbunden mit einer Umsetzung in Code formeller Kriterien eine hinreichende Lösung bewirkt.

### *Fazit*

Opt-in und opt-out-Modell stellen Lösungen für das spam-Problem dar. Die Bevorzugung des einen gegenüber dem anderen Modell ist Ausfluss unterschiedlicher Präferenzen der Akteure hinsichtlich des Schutzes der Privatsphäre, letztlich der Stellung des Datenschutzes gegebenüber den Rechten Dritter, insbesondere der unternehmerischen Freiheit, die ein Recht auf Werbung impliziere.

Die USA und einige ostasiatische Staaten haben sich für ein opt-out-Modell entschieden. Die EU und die meisten übrigen europäischen Staaten haben sich für ein opt-in-Modell entschieden. Opt-in und opt-out-Modell sind vereinbar. Hierzu ist es erforderlich, dass das global opt-out-Modell funktioniert und die Interessen derjenigen des opt-in-Modells berücksichtigt. Die Struktur des Codes ist hierfür entscheidend.

Für die Staaten mit einem opt-in-Modell empfiehlt sich bereits die Einflussnahme auf die Ausgestaltung des global opt-out-Modells der USA als weltgrößtem Exporteur für spam, da sie weitgehend von der Berücksichtigung ihrer Interessen durch die USA abhängig sind. Allerdings ist eine Berücksichtigung dieser Interessen auch im Interesse der USA. Die Ausgestaltung und Implementation – ggf. auch das Scheitern – des global opt-out-Modells können als richtungsweisend für die weitere politisch-rechtliche Bekämpfung von spam angesehen werden.

Da die Implementation des global opt-out-Modells abgewartet werden muss und Verhandlungen über eine Berücksichtigung der Erfordernisse des opt-in-Modells noch nicht begonnen haben, ist mit keiner schnellen Lösung zu rechnen. Meiner Schätzung nach nicht vor 2008, es sei denn Innovationen treten ein, die das spam-Problem besei-

tigen. Ansätze könnten in einer Stärkung der Echtheit von Informationen (formeller Kriterien) bestehen, die das Filtern erleichtern, wie zum Beispiel dem Absender einer Email.

Das Scheitern einer kooperativen Lösung für die Vereinbarkeit von opt-in- und opt-out-Modell kann zur weltweiten Etablierung des opt-in-Modells führen. Alternativ - und wahrscheinlicher – bestärkt es eine Entwicklung, die zu noch mehr Kontrolle und in seiner Folge weniger Anonymität führt.

Wird diese als Wert angesehen, dann ist die kooperative Lösung zur Vereinbarkeit von opt-in- und opt-out-Modell deutlich zu bevorzugen, da sie ein höheres Maß an Anonymität zu gewährleisten scheint.
Auch ist die Lösung die einzige, die alle weitestgehend von den Kosten des spam in ihrem jeweiligen Verständnis befreien dürfte.

Die Lösung Bedarf verzichtet nicht auf andere Lösungsansätze, wie die Filtertechnik Insbesondere wird ihr ein weiter Rolle in einem multi-dimensionalen Ansatz zukommen, allerdings dürfte sie aus dem Fokus des öffentlichen Interesses verschwinden. In der Übergangszeit wird sie das einzige Mittel darstellen, das spam-Problem zu lindern.

Da Ansätze zu Gesprächen über das spam-Problem im Rahmen der OECD gesichtet werden, stelle ich es in Frage, ob diese insbesondere vor dem Hintergrund des Zusammengehens von Viren und spam in 2003 noch das geeignete Gremium sind. Als Ursprungsländer für Trojaner und Viren, die eine illegale Infrastruktur für spamming schaffen stehen Russland und weniger entwickelte Länder - insbesondere in Osteuropa und auf dem Balkan - in Verdacht, die gerade nicht Mitglied der OECD sind.
Die Wahl einer Organisation hat hier natürlich nicht nur Einfluss auf die beteiligten Akteure, sondern auch auf den Verhandlungsmodus und die Strategien.

Zum Schluss sei der Hoffnung Ausdruck verliehen, dass die offenbar nötige Intervention des Staates bzw. der Staaten nicht den Auftakt weiterer Regulierungen darstellt, die zu mehr Kontrolle des Cyberspace führen.

# Literaturverzeichnis

Das es sich bei 'spam' um ein Problem des Internets handelt, wundert sicher nicht, dass die überwiegende Zahl der Dokumente hierzu online vorliegt. Auf eine Trennung der online-Dokumenten von übrigen Publikation wurde verzichtet, erste wurden zur Kenntlichmachung kursiv abgedruckt.

Um der Komplexität und Vielzahl an Quellen Herr zu werden, wurde für diese Arbeit systematisch das Wired News Magazine ausgewertet, aus dem nun der Großteil der Quellen stammt. Online-Magazine wie Wired News Magazine, Telepolis und Internet Intern wurden übrigen Webseiten vorgezogen.


*AP 2003a:* *Associated Press; Pop-Up Go the Weasels; Wired News 16.12.2003; http://www.wired.com/news/business/0,1367,61626,00.html (zuletzt 22.2.2004)*

*AP 2003b:* *Associated Press; Company Fights for Pop-Up Rights; Wired News 9.12.2003; http://www.wired.com/news/business/0,1367,61532,00.html (zuletzt 22.2.2004)*

*AP 2003c:* *Associated Press; FTC Slams Pop-Up Ad Firm; Wired News 6.11.2003; http://www.wired.com/news/politics/0,1283,61123,00.html (zuletzt 22.2.2004)*

*AP 2003d:* *Associated Press; Congress: We Don't Want Any Spam!; Wired News 24.11.2003; http://www.wired.com/news/politics/0,1283,61361,00.html (zuletzt 22.2.2004)*

*AP 2003e:* *Associated Press; Congress Votes to Can Spam; Wired News 8.12.2003; http://www.wired.com/news/politics/0,1283,61518,00.html (zuletzt 22.2.2004)*

*AP 2003f:* *Associated Press; Bush Signs Anti-Spam Bill; Wired News 16.12.2003; http://www.wired.com/news/politics/0,1283,61622,00.html (zuletzt 22.2.2004)*

*AP 2003g:* *Associated Press; Virginia Nabs Two Big Spammers; Wired News 11.12.2003; http://www.wired.com/news/business/0,1367,61567,00.html (zuletzt 22.2.2004)*

*Asaravala 2003a:* *Asaravala, Amit; Tomorrow's Menu: Spam, Spam, Spam; Wired News 11.12.2003; http://www.wired.com/news/politics/0,1283,61555,00.html (zuletzt 22.2.2004)*

*Asaravala 2003b:* *Asaravala, Amit ; Antispam Companies Raking It In ; Wired News 9.9.2003; http://www.wired.com/news/business/0,1367,60327,00.html (zuletzt 22.2.2004)*

*Asaravala 2004:* *Asaravala, Amit; With This Law, You Can Spam; Wired News 23.1.2004; http://www.wired.com/news/business/0,1367,62020,00.html (zuletzt 22.2.2004)*

*Baard 2004:* *Baard, Mark; Going Upstream to Fight Spam; Wired News 20.1.2004; http://www.wired.com/news/infostructure/0,1377,61971,00.html (zuletzt 22.2.2004)*

Baase 2003: Baase, Sara; A Gift of Fire. Social, Legal and Ethical Issues for Computers and the Internet; Upper Saddle River/New Jersey 2003

Beck 1986: Beck, Ulrich; Risikogesellschaft. Auf dem Weg in eine andere Moderne; Frankfurt/Main 1986

Becker 2003: Becker, Alexander; Google im Griff der Spam-Mafia ; in: tomorrow 10/2003; Hamburg 2001

Bohne 2002: Bohne, Andreas; Zinser, Axel F.; Porto zahlt Empfänger : Spamming: Unverlangte Werbung per News und Mail ; in: iX 3/1997, Hannover 1997

*Bruns 2003:* *Bruns, Holger; Die Verwundbarkeit der Microsoft Software. Immer mehr Rechner werden von Spammern gekidnappt; Telepolis 5.8.2003; http://www.heise.de/tp/deutsch/inhalt/te/15329/1.html (zuletzt 22.2.2004)*

*CAUCE 2004:* *CAUCE; "Won't the spammers just go offshore?"; 2004; http://www.cauce.org/about/faq.shtml#offshore (zuletzt 4.2.2004)*

*Dean 2004:* *Dean, Kari L.; Stop the Cash Flow, Kill the Spam; 6.2.2004; http://www.wired.com/news/infostructure/0,1377,62177,00.html (zuletzt 22.2.2004)*

*Delio 2002a:* *Delio, Michelle; When the Spam Hits the Blogs; Wired News 26.10.2002; http://www.wired.com/news/culture/0,1284,56017,00.html (zuletzt 22.2.2004)*

*Delio 2003a:* *Delio, Michelle; The Internet Is a Very Sick Place; Wired News 23.12.2003; http://www.wired.com/news/infostructure/0,1377,61710,00.html (zuletzt 22.2.2004)*

*Delio 2003c:* *Delio, Michelle; Spam Is in Eye of the Beholder; Wired News 4.6.2003; http://www.wired.com/news/business/0,1367,59089,00.html (zuletzt 22.2.2004)*

*Delio 2003d:* *Delio, Michelle; The Fanatasy and Reality of 2004; Wired News 29.1.2003; http://www.wired.com/news/culture/0,1284,61726,00.html (zuletzt 22.2.2004)*

*Delio 2003e:* *Delio, Michelle; Spam: This Time It's Personal; Wired News 29.9.2003; http://www.wired.com/news/politics/0,1283,60635,00.html (zuletzt 22.2.2004)*

*Delio 2003f:* *Delio, Michelle; Spam: Much Hated, Little Defined; Wired News 1.5.2003; http://www.wired.com/news/politics/0,1283,58682,00.html (zuletzt 22.2.2004)*

*Delio 2004a:* *Delio, Michelle; Spam Filters Grab Good With Bad; Wired News 19.1.2004; http://www.wired.com/news/infostructure/0,1377,61945,00.html (zuletzt 22.2.2004)*

*Delio 2004b:* *Delio, Michelle; Worm Slowing, but Still Dangerous; Wired News 28.1.2004; http://www.wired.com/news/technology/0,1282,62073,00.html (zuletzt 22.2.2004)*

*Dotinga 2003:* *Dotinga, Randy; The Cell: It's a Selling Machine; Wired News 27.9.2003; http://www.wired.com/news/wireless/0,1382,60610,00.html (zuletzt 22.2.2004)*

Ermert 2004: Ermert, Monika; Strategierunde der Anti-Spam-Krieger ; in: c't - Magazin für Computer und Technik 4/2004 (S. 32)

*EU-Studie 2001:* *Gauthronet, Serge; Drouard, Etienne; Unsolicited Commercial Communications and Data Protection; Commission of the European Communities (Hrsg.); http://europa.eu.int/comm/internal_market/privacy/docs/studies/spamsum_de.pdf (zuletzt 22.2.2004)*

*EuroCAUCE:* *EuroCAUCE; Opt in vs. Opt out; http://www.euro.cauce.org/en/optinvsoptout.html (zuletzt 22.2.2004)*

*Fallows 2003:* *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)*

*Ferris 2003a:* *Ferris Research; Research Focus: Spam; http://www.ferris.com/pub/FR-126.html (zuletzt 22.2.2004)*

*Ferris 2003b:* *Ferris Research; Cost of Junk Email to Exceed $10 Billion for American Corporations in 2003; Pressemitteilung 6.1.2003; http://www.ferris.com/pub/FR-126.html (zuletzt 22.2.2004)*

Fischer 2004: Fischer von Mollard, Michael; Ungerer, Bert; "Sender Permitted From" gegen Spam ; in: iX 3/2004; Hannover 2004

*FTC 2002:* *FTC - Office of Consumer and Business Education; You've Got Spam: How to "Can" Unwanted Spam; April 2002; http://www.ftc.gov/bcp/conline/pubs/online/inbox.pdf (zuletzt 22.2.2004)*

*FTC 2003:* *Federal Trade Commission; FALSE CLAIMS IN SPAM; 30.4.2003; http://www.ftc.gov/reports/spam/030429spamreport.pdf (zuletzt 22.2.2004)*

*Glasner 2001:* *Glasner, Joanna; A Brief History of SPAM, and spam; Wired News 26.5.2001; http://www.wired.com/news/business/0,1367,44111,00.html (zuletzt 22.2.2004 )*

*Glasner 2004:* *Glasner, Joanna; Open Up a Can of Spam; Wired News 16.1.2004; http://www.wired.com/news/politics/0,1283,61928,00.html (zuletzt 22.2.2004 )*

Gleick 2003: Gleick, James; You have spam ; in: The New York Times Magazine 9.2.2003

*Graham 2003a:* *Graham, Paul; Will Filters Kill Spam?; Dezember 2002; http://www.paulgraham.com/wfks.html (zuletzt 31.10.2003)*

*Graham 2003b:* *Graham, Paul; Stopping Spam; August 2003; http://store.yahoo.com/paulgraham/stopspam.html (zuletzt 22.2.2004)*

*Heinzmann 2002:* *Heinzmann, Peter, "Datenschutz Aktuell" Spamming, Spying, P3P; Datenschutz Forum Schweiz; Rapperswill/Schweiz 2002 http://www.datenschutz-forum.ch/veranstaltungen/unterlagen/spam.pdf (zuletet 22.2.2004)*

Ingham 2003: Ingham, Jenni; E-mail overload in the UK workplace ; in: Aslib Proceeding: New Information Perspectives 3/2003

*Intern 2003a:* *Internet Intern; Comment Spam; 28.10.2003; http://www.intern.de/news/4916.html (zuletzt 22.2.2004)*

*Intern 2003b:* *Internet Intern; Darf AOL das?; 24.10.2003; http://www.intern.de/news/4908.html (zuletzt 22.2.2004)*

*Kernaghan 2003:* *Kernaghan, Kenneth; Riehle, Nancy; Politicians' Use of ICTs: A Survey of Federal Parliamentarians; 2003; http://www.publicsectorit.ca/publications/CBStudy.pdf (zuletzt 20.2.2004)*

Koser 2004: Koser, Wolfgang; „Macht E-Mail teurer!“ ; in: Internet professionell 2/2004; München 2004

Lee 2003: Lee, Jennifer 8.; We Hate Spam, Congress Says (Except Ours); The New York Times 28.12.2003

Lessig 1999: Lessig, Lawrence; Code und andere Gesetze des Cyberspace; Berlin 1999

*Lutus 2003:* *Lutus, Paul; The Anti-Spam Home Page; 3.7.2003; http://www.arachnoid.com/lutusp/antispam.html (zuletzt 22.2.2004)*

*McWilliams 2003:* *McWilliams, Brian; Blackmailed by Pop-Up Advertising; Wired News 22.9.2003; http://www.wired.com/news/business/0,1367,60509,00.html (zuletzt 22.2.2004)*

Medosch 2001: Medosch, Armin; Einen Hoax will er sich machen; in: Medosch, Armin; Röttgers, Janko (Hrsg.): Netzpiraten: Die Kultur des elektronische Verbrechens; Hannover 2001

Mitnick 20003: Mitnick, Kevin; Simon, William; Risikofaktor Mensch. Die Kunst der Täuschung.; Bonn 2003

Norman 1999: Norman, Donald A.; The Invisible Computer; Cambridge,/USA, London 1999

*NZZ Online 2003:* *Spam auf der Anklagebank; in: NZZ Online (Neue Zürcher Zeitung) 20.6.2003 http://www.nzz.ch/netzstoff/2003/2003.6.20-em-article8XD4G.html (zuletzt 22.2.2004)*

*OECD 2004:* *OECD, Background Paper For the OECD Workshop on spam; 2.2.2004; http://www.olis.oecd.org/olis/2003doc.nsf/LinkTo/dsti-iccp(2003)10-final (zuletzt 22.2.2004)*

*PEW 2004:* *PEW Internet and American Life Project; Cable and Internet Loom Large in Fragmented Political News Universe: Perceptions of Partisan Bias Seen as Growing; 11.1.2004; http://www.pewinternet.org/reports/pdfs/PIP_Political_Info_Jan04.pdf (zuletzt 20.2.2004)*

*Reuter 2003e:* *Reuters; Senate Bill Sticks It to Spammers; Wired News 2003; http://www.wired.com/news/politics/0,1283,61343,00.html (zuletzt 22.2.2004)*

*Reuters 2003a:* *Reuters; MS Calls Out Bounty Hunters; Wired News 5.11.2003; http://www.wired.com/news/politics/0,1283,61086,00.html (zuletzt 22.2.2004)*

*Reuters 2003b:* *Reuters; Spammers Tap Unwitting Users' PCs; Wired News 3.12.2003; http://www.wired.com/news/technology/0,1282,61457,00.html (zuletzt 22.2.2004)*

*Reuters 2003c:* *Reuters; Windows 'Feature' Draws FTC's Eye; Wired News 5.11.2003; http://www.wired.com/news/business/0,1367,61113,00.html (zuletzt 22.2.2004)*

*Reuters 2003d:* *Reuters; New Virus Dresses Up As E-Mail; Wired News 31.10.2003; http://www.wired.com/news/technology/0,1282,61042,00.html (zuletzt 22.2.2004)*

*Reuters 2003e:* *Reuters; Worm Aims to Disarm Spam Fighters; Wired News 2.12.2003; http://www.wired.com/news/technology/0,1282,61434,00.html (zuletzt 22.2.2004)*

*Roth 2004:* *Roth, Wolf-Dieter; Spam, Betrug und Drogen; Wired News 2.2.2004; http://www.heise.de/tp/deutsch/inhalt/te/16665/1.html (zuletzt 22.2.2004)*

*Rötzer 2004:* *Rötzer, Florian; Die politischen Meinungsführer findet man im Internet; 9.2.2004; http://www.heise.de/tp/deutsch/inhalt/te/16717/1.html (zuletzt 20.2.2004)*

Scharpf 2000: Scharpf, Fritz W.; Interaktionsformen. Akteurzentrierter Institutionalismus in der Politikforschung; Opladen 2000

Schenk 1997: Schenk, David; DATA SMOG – Surviving the information glut; London 1997

Schneider 2001: Schneider, Florian; Werde reich, glücklich und satt!; in: Medosch, Armin; Röttgers, Janko (Hrsg.): Netzpiraten: Die Kultur des elektronische Verbrechens; Hannover 2001

Schwartz 1999: Schwartz, Alan; Garfinkel, Simson; Stoppt Spam - kurz & gut; Köln 1999

*Singel 2003:* *Singel, Ryan; Spam Pitches Are Mutating Faster; Wired News 28.1.2003; http://www.wired.com/news/infostructure/0,1377,60941,00.html (zuletzt 22.2.2004)*

*Spamhaus:* *Spamhaus; The Definition of Spam; 2002; http://www.spamhaus.org/definition.html (zuletzt 22.2.2004)*

*Sweet 2003:* *Sweet, Mark; POLITICAL E-MAIL: PROTECTED SPEECH OR UNWELCOME SPAM? ; in: Duke Law & Technology Review 14.1.2003; http://www.law.duke.edu/journals/dltr/articles/PDF/2003DLTR0001.pdf (zuletzt 22.2.2004)*

*Ulbrich 2004:* *Ulbrich, Chris; Spam Travels Into Gray Area; Wired News 29.1.2004; http://www.wired.com/news/technology/0,1282,62087,00.html (zuletzt 22.2.2004)*

*VeriSign 2003:* *VeriSign; A Plan for No Spam; 2003 www.verisign.com/resources/wp/spam/no_spam.pdf (zuletzt 22.2.2004)*

Wang 2003: Wang, Wallace; Steal This Computer Book 3. What They Won't Tell You About the Internet; San Francisco/USA 2003

Winkel 2000: Winkel, Olaf; Sicherheit in der digitalen Informationsgesellschaft. IT-Sicherhiet als politisches, ökonomisches und gesellschaftlichs Probelm ; in: Aus Politik und Zeitgeschichte 41-42/2000

*Wired News 2003a: Wired News Report; Breaking News: Most Spam Is Bogus; Wired News 29.4.2003; http://www.wired.com/news/business/0,1367,58664,00.html (zuletzt 22.2.2004)*

*Wired News 2003b: Wired News Report; Cyber Sweep' Nets 125 Arrests; Wired News 20.11.2003; http://www.wired.com/news/business/0,1367,61317,00.html (zuletzt 22.2.2004)*

*Wired News 2003c: Wired News Report; Blockbuster Woes, Netflix Gains - Spam costs billions; Wired News 3.1.2003; http://www.wired.com/news/business/0,1367,57054,00.html (zuletzt 22.2.2004)*

*Zetter 2004:* *Zetter, Kim; Kazaa delivers more than tunes; Wired News 9.1.2004; http://www.wired.com/news/business/0,1367,61852,00.html (zuletzt 22.2.2004)*