16-July-2003

SPAM

What Are the Legal Implications?

Authors:

Michael Biggs	mbiggs@surfr.com
Quasedra Mobley	qmobley@comcast.net
Anthony Mitchell	mitchea@excite.com
Pam Cote	pam@pcexpressions.com
Tyler Maciolek	tylerm23@softhome.net

Table of Contents

Introduction

This paper provides a global snapshot of what has quickly developed into a global problem: the proliferation of unsolicited commercial e-mail (UCE, aka SPAM). The impact of SPAM affects companies and consumers alike as they find inboxes stuffed on a daily basis with unwanted solicitations for products and services ranging from Viagra, to home refinancing, to "get rich quick" schemes, to pornography, to invitations from 3rd World politicians to help them launder money. Processing UCE takes time, consumes bandwidth, invades privacy, interferes with legitimate commercial and private communications, and subjects recipients to the risk of viruses, worms, and Trojan horses should they be momentarily distracted by and open a seductive subject line. UCE generally uses false return address headers, which makes tracing their origins difficult if not impossible. It can truthfully be described as the pollution or contagion of the Internet that interferes with legitimate commerce and discourages computer users from taking advantage of this revolutionary form of global communication. Indeed, SPAM is perhaps the world's ultimate SCAM as the technological architecture of the Internet provides hucksters immediate access to millions of people while (this is the rub) passing all of the social, administrative, and infrastructure costs to the recipients.

The SPAM epidemic has reached such proportions that local and national governments are finally feeling pressure to do something about it. In this paper, we catalog the harm caused by SPAM; describe the communications protocols that technologically enables the epidemic; survey the muted

attempts to date by U.S. state and Federal governments and the European Community (EU) to address the problem; and, based on this insight, construct a politically feasible model for UNCITRAL for addressing the global control of what is a global problem. As we shall see, discussions about the best approach to regulating SPAM can quickly become disingenuous for a number of reasons. There is not a universally accepted definition for it. Is it *all* unsolicited e-mail, or just those e-mails the recipients, after the fact, find personally offensive? How do you regulate *who* can send *what* to *whom* on the Internet, given the Internet's legacy of operating without regulation (a freedom that, at least in the U.S., has found some basis in Constitutional law)? Politically, how can governments intervene against vested business interests to proscribe a revolutionarily low-cost way of finding and communicating with millions of potential customers? As a business manager, how do you weave the fine line between using e-mail as a legitimate commercial activity, avoid being categorized as an anti-social spammer, or, at worst, avoid running afoul of the law? Let's look at these issues in more detail.

Proof of Harm

What is SPAM? Ask any e-mail user and they will tell you that SPAM interrupts their work, wastes time, and makes them afraid to use their e-mail address in public. There is a miasma of definitions depending upon your point of view. Most will agree with Bill Gates and Brad Templeton that SPAM is the pollution of the Internet and e-commerce. The most universal agreement is on the point that it is unsolicited. The California state statute defines "unsolicited e-mail documents" as "any e-mailed document or documents consisting of advertising material for the lease, sale, rental, gift offer, or other disposition of any realty, goods, services, or extension of credit."[1]

UCE is unsolicited commercial e-mail, and UBE, unsolicited bulk e-mail and is perhaps closer to the popular definition. Brad Templeton, creator of the first Internet newspaper, ClariNet, defines

SPAM as a mass mailing to a group of people to whom you are a stranger, and who did not request the mailing.[2] This can include religious proselytizers who threaten death will come to you if you don't subscribe to their brand of worship, political agitators who blanket the public with anonymous opinions, and those sending child pornography for thrills. But it can also mean the family reunion organizer trying to reach relatives they have never met, or a school band booster compiling e-mail addresses from your children to send practice schedules by e-mail. Paul Soltoff writes that SPAM "is an e-mail message that the recipient -- and only the recipient -- deems inappropriate, unwanted, or no longer wanted for any reason."[3] As far back as September 1990, a message board conversation recorded, "It has been generalized to mean sending lots of crap to servers as well as people you want to annoy the hell out of."[4]

A search of the etymology of SPAM reveals a link to the 1987 Monty Python SPAM Sketch from "The Final Rip Off" and other albums as well as preformed on episode 25 of Flying Circus TV Show.[5] A waitress tells Vikings what is on the menu and everything includes SPAM. When a couple of lawyers sent a message to every newsgroup on USENET in April 1994, it was related to the skit and became common usage. After several years of supporting SPAM as a legitimate advertising vehicle, the Direct Marketing Association finally accepted that SPAM is a problem. Their anti-SPAM strategy document favors a method of handling SPAM by using "opt-out".[6]

---

1 State of California, Business and Professions Code Section 17530-17539.6 17538.4. (a).
2 Brad Templeton, *Essays on Junk E-mail (Spam)*, <http://www.templetons.com>, visited 7/14/03.
3Paul Soltoff, *Searching for a Definition of Spam*, November 4, 2002 <http://www.clickz.com/em_mkt/em_mkt/article.php/1492521>, visited 7/14,03.
4 Brad Templeton, *Origin of the term "spam' to mean net abuse*, <http://www.templetons.com/brad/spamterm.html>, visited 7/14/03.
5 Jonathan Partington, *The Original Monty Python SPAM Skit*, Transcribed September 17, 1987 from "Monty Python's Previous Record", <http://home.triad.rr.com/spamchef/spamskit.html>, visited 7/14/03.
6 The Direct Marketing Association, *Anti-Spam: Direct Marketing Association Anti-Spam Working Strategy*, May 27, 2003, <http://www.the-dma.org/stopspam/workingstrategy.shtml>, visited 7/14/03.

Some Terminology

1. ***Email Append***: A method of compiling e-mail lists by using non-email lists with name, address, phone number, etc., (such as from the pizza delivery) and matching them up to other lists with e-mail addresses in order to create e-mail master lists.

2. ***Joe-Jobs***: Spamming under the forged identity of competitors with intent to harm the competitors' reputations.

3. ***Morphing***: Creating nonsense subjects using a random generator to make each e-mail unique.

4. ***Spoofing***: E-mails that are made to appear as though they come from an employee of a trusted company with a legitimate e-mail address.

5. ***Trojan***: A virus sent to computers for the purpose of accessing those computers for distribution purposes.

What is the Real Harm?

Existing Federal and State laws that have been used as a basis for lawsuits in the U.S. include unauthorized use of resources, forgery, impersonation, trespass, fraud, computer crime, trademark infringement, and illegal telecommunications solicitation. Some cases that may have legal grounds for prosecution or have been prosecuted are described below:

- **Defamation:** There are cases of malicious dissemination of myths and urban legends, spreading biased information.

- **Theft of Identity:** A recent example occurred when emails were sent to Best Buy customers as well as people with no connection to the company, that claimed to be from BestBuy.com's Fraud Department and asked for personal information such as Social Security numbers and credit card information."[7]

- **Loss of Business:** ISP's are losing customers whose major reason for signing up was to use e-mail. They close their accounts when e-mail is no longer of value to them. The ISPs also spend time dealing with customer complaints, tuning filters to eliminate SPAM, and teaching customers how to use filters, costing hundreds of thousands of dollars.

- **Crimes Against Children:** Filtering technologies may appear to be the answer, but the problem cannot be solved simply by putting software onto the family PC. John Carr, Internet consultant for children's charity NCH, points out that children's safety is a major

7 Benno Groeneveld, The Business Journal, Best Buy hit by fraudulent SPAM e-mail, June 19, 2003, <http://twincities.bizjournals.com/twincities/stories/2003/06/16/daily35.html>, visited 7/14/03.

concern as the Internet becomes increasingly mobile with the onset of next generation mobile handsets. He said, "Children's mobile phones are their most prized possessions".[8] There isn't a method of filtering images on either the home PC or the picture phone because the software searches for words. It can't tell whether a picture is offensive.

- **Fraud:** A Washington state law (March 1998) bans all unsolicited commercial e-mail sent by or to Washington residents with misleading subject lines, false transmission paths or phony return addresses. The Supreme Court compared this type of SPAM to getting junk mail with a postage-due notice on it because it can't be traced and costs everyone money except the sender.

- **Chain Letters:** According to the FTC, if chain mail "promises any kind of return – like money – it's fraudulent and illegal! If you start or forward one, you could face legal action."[9]

- **Scams:** "Deceptive schemes and illegal scams including auction fraud, the illegal sale of controlled substances, bogus business opportunities, deceptive money-making scams, illegal advance-fee credit card offers, and identity theft" are being prosecuted.[10]

- **Trespass:** McAfee.com tracked a large and increasing number of password-stealing trojans infecting AOL users. "APStrojan.qa" spreads through e-mail, often carrying the message "hey you" and installs itself on users' systems, while attempting to steal AOL version 4.0 and 5.0 user account names and passwords and forward them. It then attempts to replicate itself to active AOL screen names listed in the infected user's "Buddy List." This trojan was designed to provide unauthorized access to victims' AOL user accounts, including e-mail.[11]

- **Privacy Abuse:** This occurs when an e-commerce or charity offers their email lists for sale, especially when their privacy policy states that they won't. In other cases, a web shopping cart supplier may have a notice that any e-mail information will be subject to sharing, but the e-commerce websites who use the shopping cart service may not reproduce that notice; or if the user finds it, it is in tiny print and therefore ignored.

What does SPAM Cost?

Everybody pays for SPAM but the sender. Larry Donahue, COO for the Albuquerque Web hosting company FatCow, says "The whole issue with SPAM is cost shifting -- spammers are

8 Will Sturgeon, Spam *Summit: Is it too late to save the kids?,* 2 July 2003, <http://www.silicon.com/news/165/1/4959.html?nl=20030703>, visited 7/14/2003.
9 *FTC Spam Scams,* <http://www3.ftc.gov/bcp/conline/edcams/spam/coninfo.htm>, visited 7/14/03
10 Federal Trade Commission, *Law Enforcement Posse Tackles Internet Scammers, Deceptive Spammers*, May 15, 2003 <http://www3.ftc.gov/opa/2003/05/swnetforce.htm>, visited 7/14/03
11 Security ASP warns AOL users of trojan, February 2, 2001, <http://www.out-law.com, search words "trojan">, visited 7/14/03

collecting millions but the cost is on CLECs, ISPs, hosting providers and ultimately, consumers".[12] A Louisiana spammer told the Senate Commerce Committee that he could send 180 million e-mails every 12 hours. Donohue estimates SPAM is 60% of the 3 million e-mail pieces the company handles each day and costs $100,000 per year to handle.[13]

SPAM is costing $8.9 billion to U.S. corporations, $2.5 billion for European businesses, and another $500 million for U.S. and European service providers, according to a study by Ferris Research in January 2003.[14] According to Nucleus Research, the cost per corporate employee is $874 per year due to simply processing and weeding out SPAM in order to find legitimate business messages. There are additional costs when a company adds filters purported to reduce SPAM costs as much as 25%, as well as network administration activities, training employees how to use filters, and delays and non-receipt because filters are too aggressive. NR estimates that one IT person is needed to handle SPAM for every 690 e-mail boxes.[15] MessageLabs tells us that in June 2003, the global ratio of SPAM in email was 1 in 2.6 or 34.4%, and nearly 60-70% of SPAM is now sent through "hijacked" open relay (or open-proxy) computers.[16]

Cell phone users in the U.S. are paying for calls related to text messaging. While the sender of e-mail to a cell phone costs nothing to the sender, consumers are paying for the connection time to retrieve them. Additionally, cell phone users are finding their size-limited mailboxes clogged with unwanted SPAM.[17] In a case that occurred in Scotland, a spammer sent innocuous-looking text messages, usually purporting to be from a friend. " When the victim replies, they are automatically

---

12 Andrew Webb, *Fighting Spam: New Mexico Web companies weigh in on uphill battle,* New Mexico Business Weekly, June 30, 2003, <http://www.bizjournals.com/albuquerque/> search word "spam", visited 7/14/03

13 ibid

14 Mitch Wagner, Reports: *Spam Costs $11.9 Billion; Users Favor Legal Ban* January 3, 2003 <http://www.internetweek.com/story/showArticle.jhtml?articleID=6000048>, visited 7/14/03.

15 Nucleus Research, Research Note D59, Spam: The Secret ROI Killer, <http://www.nucleusresearch.com/> search word "d59", visited 7/14/03.

16 Business Editors/High-Tech Writers, *MessageLabs Intelligence Data for June 2003 Indicates Email Represents an Increasingly Serious and Complex Risk to the Enterprise, NEW YORK*--(BUSINESS WIRE)--June 30, 2003, <*http://www.businesswire.com/cgi-bin/cb_headline.cgi?&story_file=bw.063003/231815462&directory=/google&header_file=header.htm&footer_file*>, visited 7/14/03.

subscribed to a premium rate texting service. In one case, the victim was flooded with 25 texts at £1.27 each in just 24 hours, running up a £34 bill."[18]

Officials of UPS are suing because of thousands of e-mails sent to UPS customers with fake e-mail headers. They appeared to have come from UPS. This type of spoofing makes the recipient feel that they can't ignore the message because it comes from a trusted company they may have done business with in the past and they assume it is legitimate. "Companies know that something has to be done about this, and that they need to protect their corporate image. You're going to see more companies do this in the coming years," relates Mike Van Bruinisse, vice president of business development and sales for Atlanta-based CipherTrust Inc., which makes anti- SPAM and e-mail security products.[19] AOL, EarthLink, and MSN have resorted to private litigation. Last year EarthLink sued spammers for trespass, breach of contract, and violations of the Computer Fraud and Abuse Act.

Opt-Out Abuse

Lawmakers and advertisers are vying over the best method for an email user to get rid of SPAM. Most advertisers believe they should have a first shot for free, and then the user can opt out by replying to the first message that they don't want to receive any more. This is different from "opt-in" where the user must request to be added to the mailing list, and there is even a "double opt-in" where the e-mail address used during registration receives a message asking for an okay.

What is wrong with opt-out? One e-mail list manager may sell your e-mail address to 500 companies who send spam, or have it sent by the list manager. The recipient must then opt-out of 500

---

17 Wendy Lee, Spam e-mailers take aim at cell phones, Houston Chronicle, June 29, 2003, <http://pqasb.pqarchiver.com/orlandosentinel/ search words "spam cell phones"> visited 7/4/03 (paid archive, free summary).
18 IAN JOHNSTON, *Mobile users fleeced by sex line spam*, Scotland on Sunday, June 29, 2003, <http://www.scotlandonsunday.com/uk.cfm?id=711012003>, visited 7/14/03.
19 Mary Jane Credeur, UPS files suit against spammers, June 30, 2003 <http://atlanta.bizjournals.com/atlanta/stories/2003/06/30/story4.html>, visited 7/14/03.

lists. The buyer of the list may have several companies and may sell the list to another list manager who resells the list. It becomes impossible for the recipient, once identified, to keep up with the op-out. And there is no guarantee that the opt-out will be honored, or that the company won't change their sender name periodically so that they can require new opt-out messages. This doesn't take into account messages that have instructions in a foreign language.

Citibank's parent, Citigroup Inc., requires customers of any of its hundreds of affiliates to tell each one that it wants to stop receiving marketing messages. Citibank has been the object of more than 30 complaints to the Federal Trade Commission over the past year by consumers charging that the company has failed to honor their requests to remove their names from lists, or made it nearly impossible to do so.[20]

Review of Technological Environment

To better understand the problem of SPAM, it is necessary to examine the mediums that spam uses. E-mail originated in 1971 as a way for individuals working on ARPANET (the Internet precursor) to leave messages for one another. E-mail quickly became the leading application of ARPANET, making up seventy five percent of its traffic. Today, e-mail is still considered one of the leading Internet applications, resting on the foundation of two protocols. Post Office Protocol and Simple Mail Transfer Protocol are the underlying technologies that make e-mail work[21]. To understand e-mail, it is necessary to understand these protocols.

POP3

---

20 Jonathan Kim, *Web Firms Choose Profit Over Privacy*, http://www.washingtonpost.com/ac2/wp-dyn/A54888-2003Jun30?language=printer, Washington Post Staff Writer, Tuesday, July 1, 2003; Page A01, visited 7/1/2003.
21 Todd Campbell, "*The First E-Mail Message*", PreText Magazine, March 1998 http://www.pretext.com/mar98/features/story2.htm, visited 7/5/2003.

The Post Office Protocol – Version 3 (POP3) was published in RFC (Request For Comments) 1939 in May of 1996. The authors of this document explained that it was currently unreasonable to expect smaller nodes, specifically workstations, to have a local mail server on it that was constantly running and connected. Instead, there needed to be a centralized server that stored e-mail that workstations could sign into and retrieve. The Post Office Protocol was intended to be the way that workstations would access their e-mail. When a workstation connected to the network (including possibly the Internet), an e-mail client would connect to the mail server and send commands identifying the user. It would then retrieve a list of e-mails waiting, download them, and delete the e-mails off the server. The connection would then be broken and any waiting e-mail would be on the actual workstation. Additional commands are available for this protocol to manipulate how e-mail is retrieved, deleted and handled; however they are not within the scope of this document.

SMTP

The Simple Mail Transfer Protocol was published in RFC 821 in August of 1982. The objective of the protocol was to deliver e-mail across a variety of transport services in a reliable and efficient manner. Of particular importance is its ability to relay mail across different transport service environments, allowing e-mail to travel across the various systems that make up the Internet. To send e-mail, a workstation must establish a connection with an SMTP server, and identify the sender address. The workstation then specifies the recipients of the mail messages to be sent. The server verifies that it can send to the listed recipients, and then sends an indicator to the workstation specifying that it can go head and transmit all data, or that one of the recipients is rejected. After the data is sent, the server sends a reply of OK and the connection is dropped.

Relay and Authentication

During the e-mail transaction, there are two key elements that relate to SPAM. The first is the ability to relay e-mail. The majority of SMTP servers are setup to allow authorized users to send e-mail to any other system on the Internet, for example: joe@rpi.edu can use Rensselaer Polytechnic Institute's (RPI) SMTP server to send an e-mail to jane@comcast.net. The main reason a recipient would be rejected is if the host address were invalid, such as jane@comcost.com; however mail server administrators can set different standards. All in all, this is a normal operation. Now, if jane@comcast.net used RPI's SMTP server, what would happen? If RPI's server is a closed relay, she may only be able to send e-mail to an address @rpi.edu or she may not be able to send e-mail at all. Unless she can somehow prove she is an authorized user (has a network address that is part of the RPI network, for example), she is limited. However, if RPI's server is an open relay, she can send to anyone. This is what spammers often use for abuse purposes. A spammer can connect to an open relay and enter an e-mail address, such as santa@northpole.org or even a valid e-mail address (not necessarily theirs) and then send messages to any e-mail address on the Internet.[22] The server does nothing to stop this, because it is told to relay all e-mail from one address to another. As this problem became better known, mail server administrators began closing the relays, limiting access to only authorized users.

The second element is authentication. As stated before, mail servers will generally allow only authorized users to send e-mail from them. Some servers determine authorization by only allowing people on a specific network to use them (i.e. you can only use certain Internet Service Providers (ISPs) mail servers if you are connected directly to that ISP). Others rely on the sender's e-mail address, checking if it is a valid e-mail address and then allowing that person to send. However, in

22 Carolyn Meinel, "*How to Forge E-Mail", Guide To (mostly) Harmless Hacking*, Vol 1, November. 2, 2001, <http://www.happyhacker.org/gtmhh/vol1no2.shtml>, visited 6/28/2003.

March of 1999, RFC 2554 was published describing an extension to the current SMTP service that would allow authentication. Now when a workstation connects to an SMTP server, it must issue an AUTH command, identifying itself as an authorized user. Any users that failed to send an AUTH command would be locked out or limited in what they could use the server to do. However, the authentication must be actively turned on by the mail administrator and supported by the server software. While some could see the implementation of this as a way to cut down on SPAM, there are few caveats that should be explained.

One of the main issues is that this is something that needs to be implemented by the administrator. Typically, open relay systems are left that way for a reason, be it intentional or simply a lack of administrative action. Therefore, the open relays that allow SPAM would still continue on, as the administrators would probably not take the action necessary to enable this option. On the other side of the spectrum, there are administrators who are looking for a more secure form of authentication. SMTP servers transmit authentication information in plain text, so that anyone monitoring the network could capture the password and use it for themselves. To overcome this, administrators implement a different type of authentication, which may include encrypted passwords. Another reason this goes unused is that it creates more work for the user. Users generally do not wish to have to enter a separate username and password for sending mail. Instead of forcing users to do this, mail administrators will set the server to only service certain network addresses, or to rely on the authentication in POP3. For this, SMTP mail servers will check the incoming connection against the logs of the POP3 server. If the address is shown as having completed a legitimate transaction with the POP3 server, the SMTP server will allow the transaction. If no legitimate transaction occurred, the

user will be unable to send e-mail. Finally though, some administrators choose to not implement any authentication to cut down on SPAM, relying on the SPAM filters of others to block anything.[23]

Although the first 'junk' e-mail was sent on May 3rd, 1978[24] the first instance of SPAM as it is known today occurred on April 12, 1994. The message was from Laurence Canter and Martha Siegel, two lawyers who used a specially created script to post an advertisement for their firm to every newsgroup on the USENET conferencing group. This act brought up great controversy, but inspired others. Already, there were programs that people could use to send out e-mails to a massive mailing list – these were generally used for opt-in lists such as newsletters. However, marketers turned this around and began using them to send to lists of e-mail addresses that had not signed up for these e-mails.[25] The question then becomes how did these marketers find these addresses? While some ways spammers gather e-mail addresses have been covered, there are other ways that deserve some consideration.

Automation

As noted earlier, there are lists of e-mail addresses that have been verified by either the actual e-mail provider, or a third party. These lists are sold, traded or stolen by marketers to use for spamming. The lists may be generated by people signing up for another mailing list, or by websites that collect consumer information. However, the most prevalent and effective way to generate these lists is to use 'bots'. 'Bots' are programs written to scan websites, newsgroups, and e-mails for e-mail addresses and compile a list from what has been scanned. The bots are actually somewhat similar to what a search engine uses to add websites to its index, however they focus primarily on e-mail addresses. Once the list is compiled, the program may simply save a copy to be used, or it may send out a test e-

23 Robert Ratliff, personal interview, June 25, 2003.
24 Brad Templeton, "*Origin of the term 'spam' to mean net abuse*", <http://www.templetons.com/brad/spamterm.html>, visited 6/25/2003.
25 Sharal Feist, "*The father of modern spam speaks*", C|Net News.com, March 26, 200,<http://news.com.com/2008-1082-868483.html>.

mail. If the test e-mail is not returned as undeliverable, it will verify the address as being in existence. If a reply is received, this only confirms to the spammer that the address is active and in use, which can help when trying to make a list that is marketable. Once the final list is compiled, spammers will use it to send out SPAM, or sell it to other spammers.[26]

Unfortunately, once on a list, it is difficult to get off of one. While some reputable companies may SPAM (intentionally or not), they usually offer a way to opt out of future mailings, and even opt out when providing your information on their website. Most spammers, however, do not honor opt out requests, and typically use an opt out request as a sign that an address is active. This was not always a severe issue, as the user could simply report the SPAM to the spammer's Internet Service Provider (ISP), and the ISP would put a stop to it. Now though, spammers are using techniques to forge e-mail, making it appear to come from other addresses (including legitimate and even possibly trusted addresses). Since most SMTP servers do not require authentication, it is very easy to login and send mail from santa@northpole.org for example, instead of the actual address spammer@isp.com. As restrictions or authentication features are put in place on a number of SMTP servers on the Internet, this process has become more difficult, but all a spammer needs is one open relay to harass users worldwide.

Seeing as that SPAM is a technical problem, there should be a technical solution. SPAM filters, which can be implemented at server and user level, are a solution, but by no means a complete one. SPAM filters work by scanning e-mail messages and checking against a database of blocked senders or key words. If a message contains a match against one of the database entries, it can be marked as SPAM or deleted. Generally, on the server side SPAM filters scan for blocked senders or possible viruses. E-mails that are blocked will usually be deleted and the sender will receive a notice of rejection. Virus e-mails may have the virus removed, or they may be withheld from the user. There

26 "*How do get e-mail addresses*?", CyberAngels.org, <http://www.cyberangels.org/spam/how.html>, visited 6/25/2003.

are server side SPAM filters that do check for content, such as those offered by Postini, however they are not available with all providers. This is where client side filters come into play. They generally work the same way, scanning incoming messages for blocked senders or keywords and taking the appropriate action. This all happens while the e-mail is still being transmitted, so users do not have to deal with e-mails in their inbox. Again, it is important to note that these filters are not completely effective. Blocking senders may work for some, but others will simply forge a new address and resend. In other cases, spammers will have a filter evaluate their e-mail before they send so they can tailor it to 'beat the system', as it were. Bearing all of this in mind, it is obvious that a solution to the problem of SPAM will require more than just technology.[27]

US Federal & State Attempts to Control SPAM

The legal climate created by the U.S. Constitution, which is perhaps unique to the United States, has hampered attempts within the United States to regulate or control UCE. This unique climate is created by (1) the "dormant" Commerce Clause governing interstate commerce that restricts a state's ability to reach beyond its borders to regulate the behavior of non-residents; and (2) the principle of academic freedom grounded in the First Amendment right to free speech that entails that the Internet should be free of regulation given its roots as a tool for academic research sponsored by the National Science Foundation. These constitutional obstacles make the United States an exception in the world community and, therefore, a poor model for approaches to control the global epidemic in unsolicited commercial e-mail.

27 "How does an email spam filter work?" *Spam White Paper*, Vicomsoft LTD, 2003. <http://www.spambolt.com/anti_spam_faq/email_spam_filter.html>, visited 7/2/2003.

The Constitutional Context

In developing the framework for a government of checks and balances, the Constitutional Conventions circa 1787 to 1791 gave the Federal government preeminent powers in such area as interstate commerce while protecting the states (and individual citizens after the 14th Amendment was adopted in 1868) from Federal tyranny through a Bill of Rights. The Constitution in Article 1, Section 8, Clause 3 states *"Congress shall have the power ... to regulate commerce with foreign nations, and among the several states, and with the Indian tribes."*[28] In an early case about a state law authorizing a dam across a navigable creek, Chief Justice Marshall said the state act could not be "considered as repugnant to the [federal] power to regulate commerce in its dormant state."[29] The case established the judicial principle that the Commerce Clause not only grants positive powers to Congress but also acts as a negative constraint on the states; that is, just because Congress is "dormant" in an area does not empower the states to act in the vacuum. Spammers have used this judicial principle to argue that they are free of state control and in general have discretion to conduct business as they please on the Internet until Congress acts to constrain them.[30]

But, then, can Congress constrain them? The First Amendment of the Bill of Rights states that, *"Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances."*[31] Since Congress has not yet passed legislation regulating UCE, the issue has not been enjoined in the courts. However, it is a good guess that Internet spammers will try to hide behind the First Amendment right

---

28 U.S. Constitution, http://www.findlaw.com, visited 7/7/2003.
29 Willson v. Black Bird Creek Marsh Co., 850. 2 Pet. (27 US) 245, 252 (1829), <http://www.eco.freedom.org/ac92/ac92pg0212.shtml>, visited 7/6/2003..
30 Edmund B. Burke. "*Why the U.S. Commerce Clause Matters for Internet Law*," GigLaw.com, <http://www.giglaw.com/articles/2001-all/burke-2001-07-all.html>, visited 7/11/2003.

to (commercial) free speech just as the Direct Marketers Association and American Teleservices Association have sued the Federal Trade Commission over the FTC's new "do not call" list restricting unsolicited commercial phone calls as constituting unconstitutional *"prior restraint on speech by callers in certain categories that are disfavored by the government."*[32]

The Internet & Academic Freedom

The Internet has its legacy in academia with its long tradition of academic freedom that from the beginning has been protected by the U.S. courts as a special case of the First Amendment right to free speech. In Sweezy v. New Hampshire (1957), the Supreme Court ruled that academia had to be kept safe for all types of ideas, especially those found offensive by the community at large. Speaking of the majority, Chief Justice Warren said, *"Scholarship cannot flourish in an atmosphere of suspicion and distrust ... (T)eachers and students must always remain free to inquire, to study, and to evaluate, otherwise our civilization will stagnate and die."*[33] A decade later, the Supreme Court ruled in Keyishian v. Board of Regents of the University of the State of New York (1967) that *"freedom is therefore a special concern of the First Amendment, which does not tolerate laws that cast a pall of orthodoxy over the classroom. The classroom is peculiarly the 'marketplace of ideas.'* "[34] Specifically addressing the Internet, the U.S. District Court for the Southern District of New York in the American Libraries Association v. Pataki (1997) made clear that state attempts to regulate the Internet that projected beyond state borders ran afoul of the "dormant" Commerce Clause of the Constitution. But more important, the court ruled that the Internet was a national preserve that must be marked off for special protection that, in its most extreme, could paralyze development of the Internet

---

31 Amendments to the Constitution, <http://www.house.gov/Constitution/Amend.html>, visited 6/28/2003.
32 Ira Teinowitz, *DMA Sues FTC Over "Do Not Call" List*, January 29, 2003, <http://www.adage.com/news.cms?newsId=37019>, visited 7/9/2003.
33 The Text of Sweezy v. New Hampshire found at www.findlaw.com, <http://caselaw.lp.findlaw.com/scripts/getcase.pl?navby=CASE&court=US&vol=354&page=234>, visited 7/2/2003.

altogether.[35] Later in the year, in Reno v. ACLU (1997) the Supreme Court invalidated the Federal Communications Decency Act in ruling that the First Amendment could not tolerate a blanket restriction on free speech on the Internet. Although it rejected the analogy that the Internet was like print media, it accepted that the *"Web is thus comparable, from the reader's viewpoint, to ... a vast library*[36] *including millions of readily available and indexed publications."*[37]

As outlined below, the Internet began life in the late 1960s as a tool for academic research in universities and, in spite of breaking its formal links with academia circa 1995, continues to be governed by a consortium of public interest organizations.[38] At present, in a convergence of technology and purpose, the organizations persist in resisting government regulation as they continue to attempt to operate in an environment of self-regulation not dissimilar to the collegiate atmosphere found in universities.

- In 1962 the U.S. Air Force commissioned the Rand Corporation to do a study on how to maintain command and control after a nuclear attack knocked out key command and control centers. The study recommended using "packet switching" as a way to design a self-healing network that would reroute packets around war-damaged centers until they reached their destinations.
- In 1968, the Advanced Research Projects Agency (ARPA) of the U.S. Department of Defense contracted for a packet-based ARPA-net that linked its research centers at the University of California at Los Angeles and Santa Barbara, Stanford University, and the University of Utah.
- By 1973, ARPA (now named DARPA or the Defense Advanced Project Research Agency) enhanced the Network Control Protocol (NCP) into what later became the Transmission Control Protocol/Internet Protocol (TCP/IP).
- In 1976, DARPA mandated that TCP/IP would constitute the communication protocol for the APRANET.

---

34 The text of Keyishian et al v. Board of Regents of the University of the State of New York found at <http://www.bc.edu/cgi-bin/print_hit_bold.cgi/bc_org/avp/cas/comm/free_speech/keyishian.html>, visited 7/2/2003.
35 American Libraries Association v. Pataki (S.D.N.Y. 1997) 969 F. Supp. 160, 170 (Pataki), http://www.findlaw.com. Also see "The First Amendment and the Internet." <http://www.netlitigation.com/netlitigation/cases/pataki.htm>, visited 7/9/2003. .
36 The potential of the Internet as a marketplace of ideas is demonstrated by MGMT 6750: the course if present online and all of the research references for this section are from the Internet.
37 Jonathan Wallace, *Extinguishing the CDA Fire*, <http://www.spectable.org/cda/cdanl.html>, visited 76/26/2003.
38 Dave, Kristula, *The History of the Internet*, August 2001. The summary is compiled from extensive historical material on the Internet Society website. <http://www.davesite.com/webstation/net-history.shtml>, visited 6/26/2003.

- In 1981, the National Science Foundation created its own TCP/IP-based network called CSNET and connected it to the ARPANET.
- By 1986, defense contractors had been brought into the ARPANET.
- By 1987, the National Science Foundation had taken the lead in developing Internet and network technologies.
- In 1990, the Defense Department disbanded ARPANET and moved its traffic to the National Science Foundation's new high-speed NSFNET backbone. In the same year, Tim Berners-Lee at CERN in Geneva developed a hypertext system to allow the international high-energy physics community to share information.
- In 1991, the National Science Foundation established the NREN or National Research and Education Network to interconnect universities and research centers.
- In 1992, CERN releases the World-Wide-Web (WWW) and the *Internet Society* was formed.
- In 1993 Marc Andreessen at the University of Illinois develops the first graphical user interface or web browser for exploring the WWW.
- By 1994, hundreds of thousands of hosts were added to the NSFNET. In perhaps the first commercial use of the bourgeoning Internet, Pizza Hut offered pizza ordering on its web page.
- In 1995, the National Science Foundation cut off public access to the NREN and the Internet Society took over management of a commercial variant consisting of consortiums of independent Internet Service Providers throughout the world.
- Present – The Internet continues to be governed by the *Internet Society* whose membership consists of corporations; non-profit, trade and professional organizations; foundations; educational institutions; government agencies; and other international organizations.

Although formal links to universities and the National Science Foundation were severed in 1995, the Internet as an international consortium of interconnected networks using the TCP/IP networking protocol continues to be governed by the *(I)nternet (Soc)iety* (ISOC) founded in 1992. ISOC currently has 150 organizational and 16,000 individual members in over 180 countries.[39] It constitutes a forum for resolving issues affecting the future of the Internet as well as providing the organizational home for the groups responsible for Internet infrastructure standards, e.g. the Internet Engineering Task Force (IETF), and the Internet Architecture Board (IAB). As a telling legacy of its academic roots, ISOC continues to attempt to control behavior on the Internet through net etiquette or "netiquette" based on a voluntary Code of Conduct on the

39 Internet Society, *All About ISOC*, June 27, 2003, <http://www.isoc.org/isoc/> visited 6/29/2003.

model of a professional organization (the Code is contained verbatim in Appendix A with items of interest highlighted in **blue**). Key themes in the Code of Conduct are,

- Ensure Internet access to everyone.
- Do no physical harm.
- Protect the privacy of data and information stored on the Internet and the privacy of access to information.
- Avoid communications that are false or are likely to be considered as discourteous, objectionable, malicious, unwanted, or causing unjustified loss of prestige.
- Avoid fraudulent or deceptive statements.

The Code of Conduct encourages Society members to shun other members who violate the Code. With respect to SPAM, the Society admits it is a problem (although it is hard to imagine that spammers would be members of ISOC or change their behavior if shunned by its members). ISOC offers no solutions to unsolicited commercial e-mail or other issues of public policy other than to provide a forum for debating them. On the other hand, ISOC seems to accept the inevitability of increased regulation. But as a way of warding off governmental controls, ISOC advocates an increased roll for the Internet Corporation for Assigned Names and Numbers (ICANN)[40] for resolving disputes between groups of Internet users – spammers and SPAM victims – on the model of ICANN's procedures for resolving trademark issues.

Congressional Inaction in the War Against SPAM

The U.S. Government has been the driving force behind the commercialization of the Internet as it evolved from a Department of Defense program to an international medium of commerce and communication. To date, the Government (with the help of the Federal courts) has respected the academic legacy of the Internet and has taken a hands-off approach as it resists pressures, for example, to tax Internet commerce or censor content. This reluctance to regulate

40 The Internet Corporation for Assigned Names and Numbers (ICANN) is the non-profit corporation that was formed to assume responsibility for the IP address space allocation, protocol parameter assignment, domain name system management, and root server system management functions previously performed under U.S. Government contract by IANA and other entities.

the Internet also exemplifies itself in the repeated failure of Congress to pass legislation controlling UCE. In the 106th Congress (1999 – 2000), ten bills were introduced to regulate SPAM. None of the bills were enacted.[41] In the 107th Congress (2001-2002), seven bills were introduced to regulate SPAM. None of the bills were enacted. In the 108th Congress, (2003-2004), nine bills have been introduced to regulate SPAM. To date, none of them have been enacted. The table below summarizes the major themes in these bills as an indication of the direction Congress is taking in its debates on how to control unsolicited commercial e-mail.

Congress	Reference	Internet	Mobile Telecom	Standard Labeling	Opt Out Process	Do Not Mail	No Auto Address	No False Headers	No Auto Harvest	Preempt States
				Control	Control	Control	Privacy	Control	Privacy	
108th	H.R. 2515	Y		Y(S)	Y		Y	Y		Y
	S. 1052	Y			Y			Y	Y	
	S. 877	Y			Y			Y		Y
	S. 563	Y				Y				
	S. 1293	Y						Y		
	H.R. 1933	Y		Y	Y			Y		
	H.R. 2214	Y		Y(S)	Y			Y		Y
	S. 1231	Y		Y		Y		Y	Y	
	H.R. 122		Y							
107th	H.R. 718	Y		Y(S)				Y		
	H.R. 1017	Y						Y		
	S. 630	Y			Y			Y	Y	
	H.R. 3146	Y			Y			Y		
	H.R. 2472	Y		Y(S)						
	H.R. 95	Y		Y	Y			Y		
	H.R. 113		Y							
106th	H.R. 3113	Y		Y	Y	Y		Y		
	S. 2542	Y			Y			Y		
	H.R. 2162	Y			Y			Y		Y
	H.R. 1910	Y			Y			Y		
	S. 759	Y			Y	Y		Y		Y
	H.R. 1686	Y						Y		
	H.R. 1685	Y				Y		Y		
	H.R. 3024	Y			Y			Y		
	H.R. 612	Y		FTC Regulation						
	H.R. 5300		Y							
Score Card		23	3	10	14	5	1	20	3	5
Percent		89%	11%	38%	54%	19%	4%	77%	12%	19%

Note: In the above table under Standard Labeling "Y(S)" indicated standard labeling for sexually explicit material only. Bills that called for labeling unsolicited commercial e-mail in the subject line but without standardized text such as ADV: were not listed because of the difficulty in filtering such material; that is, the provisions would be

41 Summaries of these bills with links to the texts are contained in Appendix C.

relatively ineffectual in practice. Opt out mechanisms include Terms and Conditions on ISP websites prohibiting the transport of unsolicited commercial e-mail.

An analysis of the above bills shows that Congress' consistent focus over the last three years has been on regulating UCE on the Internet to the exclusion of mobile telecommunications (an emerging issue addressed previously in the paper). It shows that Congress has also had a consistent interest in ensuring that e-mail recipients have "opt out" options with an almost universal recognition that traceability and therefore regulation is impossible if spammers use false headers or return addresses. The table suggests that the scope of the bills has been increasing over the years to cover Internet technologies such as auto-addressing or auto-generating e-mail lists from randomly generated combinations as well as auto-harvesting e-mail addresses from Internet sites using Internet "bots" or agents. Although the above bills favor "opt out" options to DO NOT MAIL lists, the impact on SPAM of the Federal Trade Commission's Do NOT CALL registry opened in July 2003 to regulate unsolicited phone advertising is of yet unknown. But most important for the purpose of comparing the approaches favored by the United States versus the European Community for the global control of SPAM, Congress without question favors the continued commercialization of the Internet by forcing consumers to take the initiative to control the amount of UCE -mail in their inboxes. Consumers must take the initiative by filtering messages based on coded subject lines, opting out of individual company marketing lists on a one-off basis, and/or opting out of some but not all marketing lists through participation in a national registry rather than, as in Europe, preventing marketing lists from being generated in the first place as an aspect of protecting privacy (see the **Control** vs. **Privacy** measures in the table).

State-Level Initiatives to Control SPAM

States have led the Federal government in initiatives to control UCE just as they did on unsolicited commercial phone calls. To date 34 states have laws regulating SPAM.[42] The table below summarizes these laws based on the same major themes used to compare Congressional bills.

State	Year	Internet	Mobile Telecom	Special Labeling	Opt Out Process	Do Not Mail	No Auto Address	No False Headers	No Auto Harvest	Long Arm
				Control	Control	Control	Privacy	Control	Privacy	
Alaska	2003	Y		Y(S)						Yes
Arizona	2001	Y		Y	Y			Y		Yes
Arkansas	2001	Y		Y(S)	Y			Y		Default
California	1998	Y		Y	Y					No
Colorado	2000	Y		Y	Y			Y		No
Connecticut	1999	Y			Y			Y		No
Delaware	1999	Y			Y			Y		Yes
Idaho	2000	Y			Y			Y		No
Illinois	1999	Y			Y			Y		No
Indiana	2003	Y		Y	Y			Y		Yes
Iowa	1999	Y			Y			Y		No
Kansas	2002	Y		Y	Y			Y		Yes
Louisiana	1999	Y	Y	Y(S)	Y			Y		Default
Maine	2003	Y		Y	Y			Y		Yes
Maryland	2002	Y			Y			Y		Yes
Minnesota	2002	Y		Y	Y			Y		No
Missouri	2000	Y			Y					Yes
Nevada	1997	Y		Y	Y			Y		Default
New Mexico	2003	Y		Y	Y					Default
North Carolina	1999	Y			Y			Y		Yes
North Dakota	2003	Y		Y	Y			Y		Yes
Ohio	2002	Y			Y			Y		Default
Oklahoma	1999	Y		Y	Y			Y		Yes
Pennsylvania	2000	Y		Y(S)	Y			Y		Default
Rhode Island	1999	Y			Y			Y		Yes
South Dakota	2002	Y		Y				Y		Yes
Tennessee	1999	Y		Y	Y			Y		No
Texas	2003	Y		Y	Y			Y		Default
Utah	2002	Y		Y	Y			Y		Default
Virginia	1999	Y			Y			Y		Yes
Washington	1998	Y						Y		Yes
West Virginia	1999	Y			Y			Y		Yes
Wisconsin	2001	Y		Y(S)						Default

42 Summaries of these laws with links to the texts are contained in Appendix D.

State	Year	Internet	Mobile Telecom	Special Labeling	Opt Out Process	Do Not Mail	No Auto Address	No False Headers	No Auto Harvest	Long Arm	
				Control	Control	Control	Privacy	Control	Privacy		
Wyoming	2003	Y						Y		Yes	
Score Card		34	1	20	29			29		8	26
Percent		100%	3%	59%	85%			85%		24 %	76 %

Note: In the above table under Standard Labeling "Y(S)" indicated standard labeling for sexually explicit material only. Laws that called for labeling unsolicited commercial e-mail in the subject line but without standardized text such as ADV: were not listed because of the difficulty in filtering such material; that is, the provisions would be relatively ineffectual in practice. Opt out mechanisms include Terms and Conditions on ISP websites prohibiting the transport of unsolicited commercial e-mail. "Long-arm" refers to long-arm statutes in which state laws cover non-residents or e-mails sent into the state from outside the state. "Yes" and "No" refer to explicit provisions of the laws either covering or not covering non-residents. "Default" refers to covering non-residents of the states because the state laws did not expressly exclude them.

An analysis of the above laws shows a propensity for the states to cover regulating SPAM based on issues of privacy. Seventy-six percent (76%) of the state laws appear to be "long-arm" statutes that either explicitly or by default applies to non-residents who send SPAM into the states from outside the state. It is questionable in light of Federal court decisions whether these laws would survive scrutiny under the "dormant" Commerce Clause of the Constitution restricting state regulation of interstate commerce, even in the absence of Federal legislation.

Three court cases have set the tone for deciding the limits on the applicability of the "dormant" Commerce Clause in setting boundaries on state laws regulating SPAM. In a case already mentioned, the U.S. District Court for the Southern District of New York in the American Libraries Association v. Pataki (1997) made clear that state attempts to regulate the Internet that exercised control over the actions of non-residents ran afoul of the "dormant" Commerce Clause of the Constitution. Although the First Amendment right to free speech was also in the petition, the court declined to address it since the New York state law was already judged as unconstitutional for extending its reach over the residents and commercial activities of neighboring states.[43] If the Pataki case set the boundaries on what was not permissible, it suggested approaches subsequently used by Washington State and California that could pass constitutional muster.

In State v. Heckel (2001), the Washington State Supreme Court reversed a lower court ruling in part based on Pataki.[44] The court rejected the precedent established in Pataki that state attempts to control UCE were *ipso facto* unconstitutional because cyberspace did not have geographical boundaries and were therefore, by definition, interference in interstate commerce. It applied a two-step process to test the constitutionality of state laws: (1) Does the law openly discriminate against interstate commerce in favor or intrastate economic interests; and (2) with respect to harm and benefits, does the law balance local interests against interstate burdens? Since the law applied only to UCE sent from servers located in Washington State to state residents and the harm was manifest in overburdening networks with traffic, the court ruled that Chapter 19 RCW of the Washington Consumer Protect Act was constitutional. In Ferguson v. Friendfinders (2002), the Court of Appeal of California, First Appellate District in California also reversed a lower court decision based on Pataki.[45] As in the Heckel case, it applied the two-step test to support the very narrowly crafted California position that Section 17538.4 of the California Business and Professions Code regulated the behavior of California companies doing business with Californians and, if the statute impacted non-residents, the impact was minor and incidental. To make its case California had to preclude the necessary and sufficient conditions for minimal connection to businesses outside the state to avoid being ensnarled in issues associated with the "dormant" Commerce Clause. It did so by restricting the law to companies (1) operating in California, (2) distributing UCE to residents of California, and (3) with servers or equipment in California.

---

43 It is the primacy of the "dormant" Commerce Clause of the Constitution established in American Libraries Association v. Pataki that suggest that state attempts to regulate SPAM as a "long-arm" statute that reaches beyond state borders are unconstitutional.

44 The text of State v. Heckel found at www.findlaw.com, <http://caselaw.lp.findlaw.com/scripts/getcase.pl?court=wa&vol=2001_sc/69416-8&invol=3>, visited 7/12/2003.

45 Ferguson v. Friendfinders, Inc., et al. A092653, San Francisco County Sup. Ct. No. 307309, January 2, 2002, <http://www.findlaw.com>, visited 7/2/2003.

U.S. Attempts to Control SPAM – Prospects for the Future

Let's draw a few conclusions about the effectiveness of state-level efforts to control UCE and the prospects for Federal legislation. There is a Catch-22 for state's living under the penumbra of the U.S. Constitution as they act to regulate SPAM. To be constitutional and avoid the legal snarls of the "dormant" Commerce Clause, state laws have to be drawn so narrowly that they are at best half measures and at worst ineffectual. The common feature of State v. Heckel and Ferguson v. Friendfinders, for example, is that the servers have to be located in the state and the UCE be sent to state residents. For the spammer, the work around is an irritant: move the servers to a neighboring state to operate under the protection of the "dormant" Commerce Clause or move to another country.

Second, the judicial rulings validating the constitutionality of narrowly drawn state laws regulating SPAM have emanated from state courts – courts that rejected precedent originally set in Federal court that state-level attempts to regulate the Internet were *ipso facto* violations of the "dormant" Commerce Clause. It is an open question how these issues will fair in Federal court if the state-level rulings are appealed on constitutional grounds.

Third, since Congress has yet to legislate against SPAM, the issue of the protections provided by the First Amendment right to free speech have also not yet had their day in court. If the free speech issues associated with Federal laws directing the filtering of Internet access to pornographic and sexually explicit content from libraries are any indication, the right of spammers to send e-mails to whomever they want when they want will eventually be argued on those grounds.

Fourth, in an ironical turn of events, it is also not clear that states have the support of all of the major players in the Internet industry in controlling SPAM. Microsoft, for example, has been a significant obstacle in lobbying against state efforts in California and Missouri to put more teeth into SPAM regulation. The reasons are economic self-interest. Companies like Microsoft, America

Online, and Yahoo are content providers as well as ISPs. They want to retain the right to SPAM their own members while leaning on the force of law to exclude most UCE from outside sources. Microsoft also is trading on the SPAM control features of its newest release of mail server and e-mail software now in beta-test as the primary rationale for users to upgrade to the newest versions. As a result, key economic forces in the Internet industry want to limit the impact of SPAM legislation to false addressing and "opt out" lists that have to be exercised by the consumer on a case-by-base basis.[46]

Finally, there is a technological convergence already discussed going on between the Internet and mobile telephone systems. Mobile telecommunication providers are increasingly offering consumers the option of accessing the Internet through their mobile telephones, including receiving e-mail. The limited bandwidth for mobile telecommunications and the fact the recipient pays for the call will likely change the name of the game in terms of the harm done by spamming. When checking e-mail through mobile phones becomes commonplace, there is the potential for SPAM to bring down mobile telephone systems because they cannot handle the volume of traffic as well as directing charges to the consumers to receive UCE that he or she does not want and did not ask for.

So, what is the prospect for effective SPAM regulation at the Federal level? In the political context, it's not good. If the battles over unsolicited commercial phone calls are any indication, the issues will be tied in knots over the First Amendment right to free speech as well perpetual lobbying by strong economic interests. There will be dissimilation over the definition of SPAM. Is SPAM e-mail with falsified return addressing, or, is it all UCE? What situations will the regulations cover? What industries will be exempt? (The recent FTC rules governing the DO NOT CALL list for unsolicited commercial phone calls exempts the insurance industry, mail order companies, *all*

46 Jonathan Krim, *Internet Providers Battling to Shape Spam Legislation*, Washington Post TechNews, July 5, 2003,

businesses that a person has done business with in the past 18 months, charitable organizations, and politicians.) But, in the technological context, regulating UCE may be inevitable as Congress is forced to act to protect the bandwidth and viability of the mobile telecommunications network from overload by unsolicited content.

European (EU) Attempts to Control SPAM

If the U.S. efforts to control SPAM have been frustrated by the Constitution at state level and inaction at the Federal level, how has the EU responded to the problem? Every country across the globe has benefited from the Internet boost. Additionally, communities have had to deal with the negative influences such as SPAM that are associated with the Internet. Many people have been annoyed, intimidated and misled by the use of SPAM or UCE. Many countries have been researching how to tackle and/or resolve this issue or at least set legal policies to minimize the use of unsolicited commercial e-mail. The European Union has implemented a number of directives that control various facets of UCE. The directives are as follow:

- **E-Privacy Directive** – 2002/58/EC, focuses on the processing of personal data and the protection of privacy in the electronic communications sector.
- **E-Commerce Directive** – 2000/31/EC, concentrates on certain legal aspects of information society services in the scope of electronic commerce.
- **Distance Contracts Directive** – 97/7/EC, focuses on protection of consumers in respect of distance contracts.
- **Data Protection Directive** – 95/46/EC, focuses on individual protection with regard to the processing of personal data and on the free movement of such data.[47]

<http://www.washingtonpost.com/wp-dyn/articles/A10414-2003Jul4.html?nav=hptop_tb>, visited 7/6/2003.

47 David E. Sorkin. *Spam Laws: European Union/EEA* [online]. <http://www.spamlaws.com/eu.html> visited 6/30/2003.

E-Privacy

By further examining the directives, a more refined understanding how the directives apply to UCE issue will be acquired. The E-Privacy Directive published in 2002 replaced the Telecommunication Privacy Directive (97/66/EC).[48] The E-Privacy Directive extended the telecommunications policies beyond the public sector into the Internet arena since the Internet provides a broader range and possibilities to distribute UCE easily. The Telecommunications Privacy Directive was limited to the telecommunication sector. The E-Privacy Directive focuses on all electronic communication regardless of technologies used. The open Internet has increased the risk to individual privacy and data. The E-Privacy Directive[49] provides companies a blueprint for communication and identifying a persons or entity. ISPs should take appropriate measures to safeguard the data transmitted or received via network communication connections (for example the Microsoft lawsuits[50] filed in Washington and United Kingdom[51]). This will assist in the protection of subscriber information and protection of privacy. It also provides the limitations for using such data when it is stored. This Directive is not prejudiced to the e-Commerce Directive relating to SPAM for direct marketing.

48 *The Official Journal of the European Communities published the Directive 97/66/EC of the European Parliament and of the Council on 15 December 1997* [online]. <http://europa.eu.int/eur-lex/pri/en/oj/dat/1998/l_024/l_02419980130en00010008.pdf> visited 7/1/2003

49 *The Official Journal of the European Communities published the Directive 2002/58/EC of the European Parliament and of the Council on 12 July 2002* [online]. <http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=en&numdoc=32002L0058&model=guichett> visited 7/1/2003.

50 Microsoft Corporation v. John Does 1-20, NO. 03 2-27981-1 SEA, NO. 03-2-27987-1 SEA, <http://news.findlaw.com/hdocs/docs/cyberlaw/msdoes12061603cmp.pdf>

51 Festa, Paul. "Microsoft takes spam fight to court." *CNET News.com.* June 17, 2003. [online] <http://zdnet.com.com/2100-1105_2-1018140.html> visited 7/2/2003.

Pruitt, Scarlet. "Microsoft to fight spam with subpoenas." *IDG News Service.* February 20, 2003. [online] <http://www.computerworld.com/governmenttopics/government/legalissues/story/0,10801,78652,00.html> visited 7/5/2003.

E-Commerce Directive

The data obtained and stored about individuals may be shared and/or sold to other parties for marketing purposes. The e-Commerce Directive (2000/31/EC)[52] regulates the freedom of information shared between States and people of Europe and is clearly established to ensure integration without borders. Although the Data Protection and Telecommunication Privacy (replaced by e-Privacy) covers the protection of individual data processing, this Directives sets the framework around the free movement of data across the open networks, which is commonly known as the Internet. It controls the distribution of unsolicited commercial e-mail or SPAM across these networks even though the freedom of movement is allowed. It prohibits the interception of such communication by any other party other than the senders and receivers. The e-Commerce Directive additionally provides legal liabilities for ISPs, which is influenced by the United States Digital Millennium Copyright Act.[53] The e-Commerce Directive Article 12 – 15 basically states that the liability regime applies regardless of illegal activities involved such as defamation, pornography, copyright or unfair trading.[54]

Distance Contract

The Distance Contract Directive (97/7/EC)[55] was implemented in 1997 to protect consumers in reference to distance contracts. It stipulates the procedures a company has to use to solicit communication with a consumer who does not wish to be contacted. The Directive ensures that consumer privacy and personal data are protected and not violated since there are other means such as

52 The Official Journal of the European Communities published the Directive 2000/31/EC of the European Parliament and of the Council on 8 June 2000. *The Official Journal of the European Communities published the Directive 2000/31/EC of the European Parliament and of the Council on 8 June 2000* [online]. <http://www.spamlaws.com/docs/2000-31-ec.pdf> visited 73//2003.
53 One Hundred Fifth Congress of the United States of America at the Second Session the *Digital Millennium Copyright Act*, *One Hundred Fifth Congress of the United States of America at the Second Session the Digital Millennium Copyright Act* [online]. <http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=105_cong_bills&docid=f:h2281enr.txt.pdf> visited 7/2/2003.
54 Michel Jaccard. *EU and Swiss perspectives on e-Commerce* [online]. August 22, 2002. <http://www.tavernier-tschanz.com>.visited 7/1/2003.
55 Directive 97/7/EC of the European Parliament and of the Council of 20 May 1997: *Directive 97/7/EC of the European Parliament and of the Council of 20 May 1997* [online]. <http://www.spamlaws.com/docs/97-7-ec.pdf> visited 7/7/2003.

the Internet to solicit communication for distance contracts.[56] Of course, there are unknown risks to a consumer's privacy and personal data as new technologies are born. Additionally, a Member State does not have to allow the selling of goods or services via distant contracts. If a lawsuit were opened that is against another party in another territory, the Member State would be held accountable since the consumer has no control over the communication.

There are exclusions to the Distance Contracts Directive. They are as follows:

- Services relating to Financials
- Automatic Vending Machines or automated commercial premises
- Telecommunications operators through the use of public pay phones
- Construction and sale of immovable property or relating to other immovable property rights (except rentals)
- Auctions
- Supplies of food stuff for daily consumption supplied to homes of consumers, residence or workplace
- Accommodations, transport and catering/leisure services.

The Distance Contracts Directive also provides policies and procedures for the consumer and supplier to adhere to ensure the rights and privacy of the consumer are not violated as well as fostering a healthy communication between the parties involved. You can view the text by examining the Article section of the Directive document.

Data Protection Directive

The Data Protection Directive (95/46/EC)[57] was implemented in 1995 to protect individuals with regard to the processing of personal data and the free movement of the data. The Directive was

56 A Distance contract is a contract concerning goods or services concluded between a supplier and a consumer under an organized distance sales or service-provision scheme operated by the supplier, who, for the purpose of the contract, makes exclusive use of one or more means of distance communication up to and including the moment at which the contract is concluded.

57 *The Official Journal of the European Communities published the Directive 95/46/EC of the European Parliament and of the Council on 24 October 1995* [online]. <http://europa.eu.int/comm/internal_market/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf> visited 7/6/2003.

designed to promote and strengthen the privacy of individuals set forth by the constitution and laws of the Member States and in the European Convention for the Protection of Human Rights and Fundamental Freedoms[58], Article 8.[59] This Directive applies to data that is processed automatically or is contained/intended to be contained in a file system such as a database for easy retrieval, and aggregation of data based by specific criteria relating to individuals. All countries or Member States are responsible for following the Directive, even if the data is processed in another country. The protection of individual privacy must be notably protected regardless of where and who processes the data. Additional to the Data Protection Directive, many countries have supported the "Opt-In" and "Opt-Out" schemas to help businesses and government agencies to control unsolicited e-mail.

Opt-In/Opt-Out

Europe has adopted "opt-in" and/or "opt-out" schemas similar to the United States. The difference is that the European Union requires companies to obtain prior approval from the consumer before they can use their information.[60] Many European countries prefer the "opt-in" schema because it requires a company to take more effort up front before sending out bulk mail. While this schema requires more work, it will keep companies out of legal situations as well as protect consumer privacy and personal data. The "opt-in" schema also provides consumers with the security of not dealing with bogus unsubscribe email addresses such as anyone@nowhere.net.

---

58 *Red the entire document on the European Convention for the Protection of Human Rights and Fundamental Freedoms* [online]. <http://www.echr.coe.int/Convention/webConvenENG.pdf> visited 7/6/2003.
Charter of Fundamental Rights in Europe [online]. <http://ue.eu.int/df/docs/en/EN_2001_1023.pdf> or <http://europa.eu.int/comm/justice_home/unit/charte/index_en.html> visited 6/27/2003.

59 Article 8 of the European Convention for *the Protection of Human Rights and Fundamental Freedoms*.

- Everyone has the right to respect for his private and family life, his home and his correspondence.
- There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

60 Richard Love and Claudia Arevalo-Love. *Identify Theft: Opt Out* [online]. 2002. <http://www.internet-tips.net/Legal/optout.htm> visited 7/1/2003.

A few European countries prefer the "opt-out" schema, but it appears that this approach makes it very difficult for the consumer to protect privacy and personal data. For this schema to be successful, the following requirements need to be met:

- Ensure all subscribers are aware or their rights;
- Simple and free to join;
- Become effective within a reasonable time of joining;
- Require companies engaged in telemarketing to update their lists regularly in the light of subscribers' notifications;
- Implement adequate complaints handling mechanisms; and,
- Support from a state supervisory mechanism.

Since countries have employed various versions of the "opt-out" schema, it may not be as effective for all industries.[61] The European Union has implemented several Directives aimed to protect consumers and control SPAM.

Conclusions & the Model UNCITRAL Law

The general conclusion that one can draw from the insights in this paper is that, at some unknown threshold, unsolicited commercial e-mail (UCE, aka SPAM) is probably here to stay. At the one extreme, we have the current situation in the U.S. in which Internet communications protocols, the "virtual space" in which it operates, and the legacy of an unregulated Internet have coalesced to make every home and business connected to the Internet a conduit for volumes of uninvited and unwanted solicitations. At the other extreme, we face the prospect of a government regulated Internet on the European model in which people are only allowed to communicate with those to have agreed ahead of time to "opt in" to receiving e-mail from strangers. But neither the anarchy of an unregulated

61 EuroCAUCE (The European Coalition Against Unsolicited Commercial Email), *Opt-In vs. Opt Out* [online]. <http://www.eurocauce.org/en/optinvsoptout.html> visited 7/8/2003.

Internet nor the draconian constraints on Internet communications "filtered" by government fiat are politically and economically viable in the long run. The most likely direction of the unfolding international dialogue on controlling SPAM is that SPAM will most likely remain a permanent and managed part of our lives as long as businesses follow a minimal set of rules while spamming their potential customers. What might those rules look like?

Foremost of all, the rules will have to be universal through a medium such as the United Nations to come to terms with the "virtual space" in which the Internet operates. Given this "virtual space," local or even national laws tend to be ineffectual. The Constitutional issues aside, state attempts in the U.S. to control SPAM are destined for failure due to the ease in which spammers can move beyond the reach of those laws by moving their servers. If local attempts at control are effectual, it is only for the short period of time it takes the spammers to make those moves. National laws face the same shortcoming. As has happened in the porn industry, local and national regulations motivate these interests to move their servers to South America, Russia, or the "wild west" of the Balkans where the laws are more favorable or, with cash paid to the right people, the law looks the other way. In the end, SPAM will have to be addressed as an international problem that affects the entire global community on the scale of international attempts to control weapons of mass destruction or bring war criminals to justice.

In the United States, the content of state laws regulating SPAM and Congressional bills that have yet to be enacted make clear that only a compromise between commercial interests that want unfettered access to potential customers and recipients who want relief from the pollution in their inboxes is politically viable. The compromise that finds almost universal acceptance is that false or misleading return addresses should be illegal to provide traceability to the source and that recipients should be able to "opt out" of marketing lists on a list-by-list basis. Spammers who do not follow

these rules are subject to legal penalty. Although this is not an ideal solution (SPAM *is* here to stay), at least it is politically viable and helps control the plague.

One suspects the same kinds of compromises will be required in the dialogue between the U.S. and EU on the way ahead to control the global epidemic in SPAM. The EU with its highly regulated societies and socialist economies will most likely not accept the free wheeling capitalism of North America and the implications that this has for an unregulated, commercialize Internet. At the same time, the United States will most likely not be able to accept the EU's draconian protection of individual privacy with its "opt in" provisions due to the Constitutional constraint that places on free speech. But, as in the state-Federal conundrum over ways to regulate SPAM, there is a middle ground in the search for minimal standards. Not surprisingly, it is the same that has been distilled from the American political experience: making it illegal to use false or misleading address headers and giving recipients an auditable way of "opting out" of marketing lists. As a minimalist approach to regulating SPAM on a global basis, this helps assure the identity of the spammer so that he or she can be held accountable to other national and local laws. It also gives all recipients options to reduce (although it will not eliminate) the volume of SPAM in their inboxes.

To help ensure SPAM is traceable to the source, the evolving international standard should also perhaps make it a fineable offense for ISPs, businesses, and private individuals to have open relays that forward SPAM. This recognizes that persons that allow open relays should bear their share of the social cost of the SPAM that they are intentionally or inadvertently facilitating. Without this minimal technical standard, international standards against false addressing and laws mandating "opt out" provisions are meaningless because they are not enforceable.

The United Nations should provide a universal standard as a mean of reaching consensus on controlling or managing SPAM. The other options (national treaties or regional consortiums) are not viable for the same reason that state laws have proved ineffectual. The spammers only have to move beyond the reach of the national or regional bodies to operate with impunity. The organizational structure and global reach for a universal standard already exists in the United Nations Commission on International Trade Law (UNCITRAL) and its Model Law on Electronic Commerce (1996). Unsolicited commercial e-mail or SPAM is by its nature an attempt at electronic commercial transactions and therefore is covered by the Model Law, especially *Chapter 15, Communication of Data Messages, Article 15: Time and Place of Dispatch and Receipt of Data Messages*.

The text of Article 15 is as follows:[62]

Article 15. Time and place of dispatch and receipt of data messages #112

(1) Unless otherwise agreed between the originator and the addressee, the dispatch of a data message occurs when it enters an information system outside the control of the originator or of the person who sent the data message on behalf of the originator. #113

(2) Unless otherwise agreed between the originator and the addressee, the time of receipt of a data message is determined as follows: #114

(a) if the addressee has designated an information system for the purpose of receiving data messages, receipt occurs: #115

(i) at the time when the data message enters the designated information system; or #116

(ii) if the data message is sent to an information system of the addressee that is not the designated information system, at the time when the data message is retrieved by the addressee; #117

62 UNCITRAL Model on Electronic Commerce (1996), Article 15. URL: http://www.jus.uio.no/lm/un.electronic.commerce.model.law.1996/15.html.

(b) if the addressee has not designated an information system, receipt occurs when the data message enters an information system of the addressee. #118

(3) Paragraph (2) applies notwithstanding that the place where the information system is located may be different from the place where the data message is deemed to be received under paragraph (4). #119

(4) Unless otherwise agreed between the originator and the addressee, a data message is deemed to be dispatched at the place where the originator has its place of business, and is deemed to be received at the place where the addressee has its place of business. For the purposes of this paragraph: #120

(a) if the originator or the addressee has more than one place of business, the place of business is that which has the closest relationship to the underlying transaction or, where there is no underlying transaction, the principal place of business; #121

(b) if the originator or the addressee does not have a place of business, reference is to be made to its habitual residence. #122

As you can see, there is a presumption in Article 15 (4a-b) that the originator must identify his or her place of business, or, if the addressee does not have a place of business, reference is made to the habitual residence.

If these articles are mandated into national and local laws, they already proscribe the false addressing behind which spammers traditionally hide their identities. To meet the remaining minimal conditions discussed earlier for controlling SPAM on a global basis, only three new provisions would have to be added to Article 15 to cover the intentional falsification of the address or origin, the phenomenon of open relays, and a minimal approach to the enforcement of "opt out" provisions. The proposed text is as follows for Article 15 (4c-e):

(c) intentional falsification of the address or habitual residence of the originator of an electronic data transaction to hide or mask the identity of #122

the originator is considered an act of commercial fraud.

(d) the maintenance of an open relay in an information system for the purpose of forwarding fraudulently addressed data messages is considered accessory to commercial fraud. #123

(e) the lack of an auditable procedure contained within the body of the data message for a recipient to opt out of receiving unsolicited and fraudulently addressed commercial data messages is considered accessory to commercial fraud. #124

The astute e-Commerce business manager needs to be cognizant of pending efforts to regulate SPAM and make ethical decisions regarding how it might be used. Our research shows that the vast majority of Internet users disapprove of SPAM, and without regulation, could actually stop using e-mail because of the waste of time, or go to a protective mode of email/using strong filters. SPAM efforts, while inexpensive, would then become useless.

Instead, the manager should concentrate efforts on being a good Internet citizen and rely on search engines and the value of the product to bring customers, who are not in their normal sphere, to the site. They should tailor their emailing lists to those who have requested to be members, use appropriate and real subjects and headers, target those with whom they already have a relationship, make it easy for them to unsubscribe, create a privacy policy that is followed, and make sure any canned integrated programs (shopping carts) adhere to a compatible privacy policy and terms of service.

While recent court cases have failed to accept the telecommunications do not call initiative applies, and have not accepted arguments that SPAM should be treated as junk mail, there will be new legislation through state and national laws in the next several years. The model legislation offered here can be used as a guideline.

When managers are conducting business either through selling goods and services or managing employees as end users, they should understand the basic and legal implications of the European Directives. The directives are setup to ensure the reasons to collect data are explicit and legitimate and there is a relevant purpose to hold the data for future analysis. Additionally, there must be an adequate level of protection when consumer personal data is transferred between countries. In case the data is transferred to another country without an adequate level of protection, the manager/company hosting the data would need to obtain consent prior to transfer. If these legal directives are not followed and consumer personal data is not protected, companies can be held liable for violating the Directive(s) and the civil rights protection laws.

Based on the European Union and United States implementation of the "Opt-Out" policy, there are obvious concerns for many companies, especially American-based. Managers of American companies need to consider the legal implications if the privacy policy is violated when conducting business in Europe. It would be advantageous for a manager to know a country's preferred approach for privacy; the opt-in or opt-out approach; when conducting business via the Internet. Using a consumer's information without obtaining prior approval violates the "Opt-In" policy in the European Union although it is not required in the United States. Managers should consider adopting the United States and European Union opt-in and opt-out policies as regular business to ensure the business relationship with other companies in various countries are preserved. Implementing both approaches will assist determine which approach is used when selling goods and services to consumers. This may cause some chaos when dealing with thousands of customers daily, but in the long term, this strategy may keep the company out of court or legal hearings.

The manager must consider the cost effectiveness of implementing filters and stay abreast of technical advances in order to reduce employee time wasted, and to provide a good work environment.

Appendix A – Internet Society (ISOC) Code of Conduct

January 2003

The original text is in English and is definitive in case of dispute about translations.

Purpose

The Internet Society's motto, for many years, has been "The Internet is for Everyone." As the Internet continues to penetrate into every corner of human society and of the economy, members of the Internet Society (ISOC) have a responsibility to demonstrate the standards of behaviour that are appropriate to continued growth and beneficial use of the Internet. People designing, building and operating Internet services, or simply using the Internet as a major tool in everyday life and work, need to adopt standards of behaviour like those of any profession. We build bridges and buildings to stand for at least 100 years, resisting natural and man-made disasters as far as possible, and to be useful for applications beyond their original design. Despite its rate of change, the Internet should be the same. Also, it should be deployed for the benefit of individuals and society, and Internet professionals have a consequent personal responsibility. Similarly, people simply using Internet services have a corresponding responsibility to avoid misuse.

The purpose of this code of conduct is to indicate the standard of professional behaviour to which ISOC members aspire, and which is intended to be an example to Internet professionals as a whole. It can be used by members to measure their own behaviour, and as a reference when considering the behaviour of others. The items in the code are intended to be as close as possible to observable or measurable behaviours, rather than requiring subjective or ethical judgment.

The code serves to define a form of professional identity. Although many aspects also apply to every user of the Internet, it is intended to give ISOC members a sense that they belong to a community with shared values and shared responsibilities.

The Code of Conduct

- When designing, implementing, operating and using Internet technology and services,
- When formulating or influencing relevant policies, laws, and regulations,
- And in all professional and personal dealings an ISOC member will

1. Take all reasonable care to ensure that his or her work and the products of his or her work cause no avoidable danger or **physical harm to any person**.
2. Take all reasonable steps to minimize waste of natural resources, damage to the environment, and damage to products of human skill and industry.
3. If his or her professional advice is not accepted, take all reasonable steps to ensure that all persons neglecting or over-ruling this advice are aware of the possible danger or damage which may result.
4. Avoid deploying technologies that defeat generally accepted technical principles of the Internet, as documented primarily by the Internet Engineering Task Force (IETF). In particular, avoid technologies that tend to subdivide access to the Internet rather than preserving its universal, unique, and international nature, except as required by security mechanisms mentioned in the next paragraph.

5. Pay particular attention to the protection of Internet services against disaster and against a physical or electronic attack, and to the **protection of the integrity and privacy of stored or transmitted information**.

6. **Take all reasonable steps, including education and the wide spreading of knowledge, to ensure the Internet can be available, accessible, and useful to everyone.**

7. Only offer or claim to offer opinions or services that lie within the member's actual knowledge or competence.

8. In the case of financial or material conflict between personal and professional interests, or between two professional interests, declare this conflict to all interested parties and if appropriate in public.

9. **Respect the generally accepted norms of Internet etiquette for human communications, especially by avoiding communications that are false or are likely to be considered as discourteous, objectionable, malicious, unwanted, or causing unjustified loss of prestige. Avoid fraudulent or deceptive statements.**

10. Respect the **rights of all Internet users to privacy of, and freedom of access to, information and communication**; promote these rights within the limits of his or her power.

11. Treat all users and colleagues fairly and on equal terms.

12. Respect legitimate intellectual property rights, do not plagiarize the work of others, and give credit to the originators of ideas.

13. Encourage others to follow this code of conduct, and discourage breaches of this code. Offer and accept honest and constructive criticisms of opinions and work as they relate to this code.

14. Not associate with, and not allow ISOC's name to be associated with, persons or organizations consistently in breach of this code.

Appendix B – Background on Internet Society (ISOC) Public Policy Activities

"There are an increasing number of sources where issues are being discussed, and decisions are being made that can and do affect the evolution of the Internet. These may stem from social, ethical, economic, political, or legal considerations, and from organizations associated within the private and/or public sectors, including industry, government, academic, or other institutions.

The Internet Society is an active member of the Noncommercial Domain Name Holders Constituency as a part of ICANN's Domain Name Support Group and will participate in deliberations regarding the domain name system and other aspects of Internet governance.

The ISOC Board of Trustees recently identified several critical areas in the public policy realm. In each case, the development and formation of a position by the Society will require analysis and debate, taking into account different regional and national views that often vary widely.

Censorship and Freedom of Expression

While the First Amendment of the U.S. Constitution is well recognized as a preeminent guiding principle of freedom of expression, it is not universally accepted. Even within the United States, there are differences of opinion as to how it should be applied. In other countries, there are historical and social issues regarding censorship and expression that must be considered.

In regard to issues of censorship and free expression, the responsibilities of service providers vary significantly from country to country.

Protection of Privacy

Data collected by service providers and Web site operators about Internet users has become a major issue both nationally and internationally. A few recent examples:

- European Union directives on privacy have conflicted with U.S. encouragement of a nongovernmental, private-sector approach.

- The control of unsolicited mail (spam) has provoked a variety of different legislative initiatives in different countries.

- There has been controversy within the IETF over possible enablement of data interception in the new protocols of IP ver 6.

- With respect to the identification of domain name holders and access to domain name databases, there is significant conflict between the interests of trademark owners in accessing the information and the privacy interests of individual domain name registrants.

Taxation

There are both international and U.S. concerns over burdensome taxation that could stifle development of the Internet as a worldwide marketplace. In the United States, there is controversy between state and federal governments arising from state concern that the traditional state revenue base of sales taxes may be destroyed by nontaxable e-commerce transactions.

Internet Governance

The Internet Society has strongly supported ICANN as the best hope of a nongovernmental approach to Internet governance. The future of ICANN depends on its ability to develop international support for its programs and to build a stable financial base. The sometimes conflicting interests of governments, of the operators of the country code top-level domains, and of various nongovernmental parties cannot be resolved without serious attention to a variety of public policy issues. These include questions about the primacy of public interest versus commercial interests, the continuing role of the Internet Society, and the continuing conflict between the needs of trademark owners and the interests of Internet users in expanding the domain name space.

Intellectual Property

Closely related to questions about Internet governance are questions about protection of trademarks. For the past five or six years, trademark issues have dominated the domain name debate. ICANN's adoption of a Uniform Dispute Resolution Policy has created an international code of trademark protection that is unprecedented in international law. While widely supported, the UDRP has also raised concerns among users of generic terms and other words or phrases that have meaning both as trademarks and in noncommercial speech.

In addition to the trademark issues, there are conflicting views on copyright issues, such as the appropriate protection of databases. For example, the European Union and the United States are pursuing different legislative approaches to database protection. Those different approaches could have serious impact on the commercial value of these database properties.

Each of the foregoing public policy issues poses a substantial challenge to the Internet Society. We hope that as time goes on, a wide range of voices and opinions will arise to develop policies that best serve the goals of the society and the Internet."

Appendix C – U.S. Congressional Bills Regulated SPAM[63]

1. Non-enacted bills in the 106th Congress (1999 – 2000):

Unsolicited Electronic Mail Act of 2000 (H.R. 3113)

H.R. 3113 would require unsolicited commercial e-mail messages to be labeled and to include opt-out instructions, and would prohibit false routing information in such messages. It would prohibit the use of a provider's facilities to send unsolicited commercial e-mail in violation of the provider's policies, if the policies are clearly posted on a web site at the domain name included in the recipient's e-mail address or are made available by an FTC-approved standard method (presumably, via the provider's SMTP server).

Originally introduced by Rep. Heather Wilson (R-NM) on October 20, 1999, with many co-sponsors (including Rep. Gene Green, sponsor of the E-Mail User Protection Act, H.R. 1910), this bill was amended in committee on March 23 and June 14, 2000, and now incorporates aspects of Rep. Gary Miller's Can Spam Act, H.R. 2162. The House of Representatives passed H.R. 3113 on July 18, 2000; it is now under consideration by the Senate.

The current version of H.R. 3113 requires "clear and conspicuous" identification of messages as unsolicited commercial e-mail, but unlike the previous version of the bill it would not require senders to use a standardized format for such labels. The original version of the bill would have required senders of unsolicited commercial or "pandering" e-mail messages to purchase an FCC-maintained exclusion list of people who did not want to receive such messages, and all unsolicited messages would have been required to include a valid reply address for opt-out requests. Providers could sue for violations of their policies on unsolicited commercial e-mail, but only after actual notice and a specific request for compliance.

Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2000 (S. 2542)

A companion bill to the Unsolicited Electronic Mail Act of 2000 (H.R. 3113), the "CAN SPAM" Act of 2000 was introduced by Sen. Conrad Burns (R-MT) on May 11, 2000. It would require senders of unsolicited bulk commercial e-mail messages to provide opt-out instructions and to honor opt-out requests. It would prohibit the use of false routing information in unsolicited commercial messages, and would prohibit the sale or distribution of software designed to falsify routing information.

Can Spam Act (H.R. 2162)

The Can Spam Act, introduced by Rep. Gary Miller (R-CA) on June 10, 1999, would prohibit using a provider's facilities to send unsolicited commercial e-mail in violation of the provider's policies, if the policies are clearly posted on a web site at the domain name included in the recipient's e-mail address or are referred to in the initial banner message displayed by the provider's SMTP server. The law also would impose criminal penalties for the unauthorized use of a third party's domain name in sending e-mail messages if it results in damage to a computer or network. State laws concerning unsolicited commercial e-mail would be pre-empted.

E-Mail User Protection Act (H.R. 1910)

63 The summaries of non-enacted bills in the U.S. Congress to control SPAM are listed at the SPAM.LAW website. The following is cited in accordance with the terms and conditions of reference: David E. Sorkin, Spam Laws, http://www.spamlaws.com/, <http://www.spamlaws.com/federal/index.html>, visited 7/13/2003.

The E-Mail User Protection Act, introduced by Rep. Gene Green (D-TX) on May 24, 1999, would make it illegal to send unsolicited bulk e-mail with a false sender's name, e-mail address, telephone number, Internet domain, or other routing information, or to distribute software designed to falsify routing information. Senders of unsolicited bulk e-mail would be required to honor opt-out requests.

Inbox Privacy Act of 1999 (S. 759)

The Inbox Privacy Act of 1999, introduced by Sen. Frank H. Murkowski (R-AK) on March 25, 1999, would require unsolicited commercial e-mail messages to include the sender's name, physical address, e-mail address, and telephone number, along with accurate routing information and opt-out instructions; senders would be required to honor opt-out requests. Owners of domain names could opt-out all addresses within a domain by registering with the FTC, although ISPs would be required to let individual customers continue receiving unsolicited e-mail at their option and to maintain and publish a list of such customers. The FTC would have rulemaking and enforcement authority; states and individual Internet providers would also be able to bring civil actions under the law. State laws concerning commercial e-mail would be pre-empted.

Internet Freedom Act (H.R. 1686)

The Internet Freedom Act, introduced by Rep. Bob Goodlatte (R-VA) on May 5, 1999, would prohibit sending unsolicited bulk e-mail with a falsified originating e-mail address, domain name, or other routing information, or to distribute software designed to falsify routing information. The bill also contains provisions that concern broadband Internet access and related services.

Internet Growth and Development Act of 1999 (H.R. 1685)

The Internet Growth and Development Act of 1999, introduced by Rep. Rick Boucher (D-VA) on May 5, 1999, would make it illegal to use a provider's facilities to send unsolicited commercial e-mail to the provider's subscribers in violation of the provider's policies. A provider could sue a sender for such violations, but only if the sender had actual notice of the policies. The bill would also make it illegal to send unsolicited bulk e-mail with a false domain name, return address, or other header information, or to distribute software designed to falsify routing information. Other provisions of the bill relate to electronic signatures, broadband Internet access, and online privacy.

Netizens Protection Act of 1999 (H.R. 3024)

The Netizens Protection Act of 1999, introduced by Rep. Christopher H. Smith (R-NJ) on October 5, 1999, would require all unsolicited e-mail messages to contain the sender's name, physical address, and e-mail address, along with opt-out instructions. False or misleading subject lines would be prohibited on unsolicited bulk e-mail messages. These requirements would not pre-empt state laws governing unsolicited commercial e-mail. Internet providers would be required to notify their customers of their policies on unsolicited e-mail, and would be able to sue customers for violations.

Protection Against Scams on Seniors Act of 1999 (H.R. 612)

Telemarketing Fraud and Seniors Protection Act (S. 699)

These companion bills were introduced by Rep. Robert A. Weygand (D-RI) on February 4, 1999, and Sen. Ron Wyden (D-OR) on March 24, 1999. They include a provision authorizing the FTC to regulate advertising that uses the Internet, including the "initiation, transmission, and receipt" of unsolicited commercial e-mail.

Wireless Telephone Spam Protection Act (H.R. 5300)

The Wireless Telephone Spam Protection Act, introduced in September 2000, would the prohibit use of wireless messaging systems to send unsolicited advertisements.

2. **Non-enacted bills from the 107th Congress (2001-2002):**

Anti-Spamming Act of 2001 (H.R. 718)

H.R. 718 was introduced in February 2001 as the Unsolicited Commercial Electronic Mail Act of 2001, by Rep. Heather Wilson (R-NM), with 67 co-sponsors. As introduced the bill was identical to H.R. 95. The bill was amended on several occasions during 2001; the version that emerged from the Judiciary Committee in June 2001 bears little resemblance to the original. The current version of H.R. 718 would prohibit false headers in unsolicited bulk commercial e-mail messages, and would require labels on sexually oriented commercial e-mail messages.

Anti-Spamming Act of 2001 (H.R. 1017)

H.R. 1017 was introduced by Rep. Bob Goodlatte (R-VA) in March 2001. It would amend federal computer crime laws to make it illegal to send unsolicited bulk e-mail messages containing a false sender address or header, or to distribute software designed for this purpose.

Controlling the Assault of Non-Solicited Pornography and Marketing (CAN SPAM) Act of 2001/2002 (S. 630)

S. 630 was introduced by Sen. Conrad R. Burns (R-MT) in March 2001. It would require unsolicited commercial e-mail messages to be labeled and to include opt-out instructions, and would prohibit deceptive subject lines and false headers in such messages. S. 630 was amended in the Senate Commerce Committee in May 2002 to include a provision prohibiting the use of e-mail addresses harvested from web sites in violation of posted restrictions.

Netizens Protection Act of 2001 (H.R. 3146)

H.R. 3146 was introduced by Rep. Christopher H. Smith (R-NJ) in October 2001; it is identical to the Netizens Protection Act of 1999, which was introduced by Rep. Smith in the 106th Congress. H.R. 3146 would require all unsolicited e-mail messages to contain the sender's name, physical address, and e-mail address, along with opt-out instructions. False or misleading subject lines would be prohibited on unsolicited bulk e-mail messages. These requirements would not pre-empt state laws governing unsolicited commercial e-mail. Internet providers would be required to notify their customers of their policies on unsolicited e-mail, and would be able to sue customers for violations.

Protect Children From E-Mail Smut Act of 2001 (H.R. 2472)

H.R. 2472 would require labels (in a format to be prescribed by the National Institute of Standards and Technology) to be included on sexually oriented commercial e-mail messages forwarded to children.

Who Is E-Mailing Our Kids Act (H.R. 1846)

H.R. 1846 would require schools and libraries that receive universal service assistance funds to adopt policies that prohibit users from sending e-mail anonymously.

Unsolicited Commercial Electronic Mail Act of 2001 (H.R. 95)

H.R. 95 would require unsolicited commercial e-mail messages to be labelled and to include opt-out instructions, and would prohibit false headers in such messages. It would prohibit the use of a provider's facilities to send unsolicited commercial e-mail in violation of the provider's policies, if the policies are clearly posted on a web site at the domain name included in the recipient's e-mail address or are made available by an FTC-approved standard method (presumably, via the provider's SMTP server).

H.R. 95, as introduced in January 2001, is identical to H.R. 3113 from the 106th Congress; in the form that bill was passed by the House of Representatives. The House Committee on Commerce published a report on H.R. 3113 in June 2000. H.R. 95 was introduced by Rep. Gene Green (D-TX), who subsequently co-sponsored another identical bill, H.R. 718.

Wireless Telephone Spam Protection Act (H.R. 113)

H.R. 113 addresses cellular phone spam. Introduced in January 2001, the bill would prohibit the use of wireless messaging systems to send unsolicited advertisements.

3. **Non-enacted bills to date from the 108th Congress (2003-2004):**

Anti-Spam Act of 2003 (H.R. 2515)

The Anti-Spam Act of 2003 was introduced on June 18, 2003, by Rep. Heather Wilson (R-NM); co-sponsors include Rep. Rick Boucher (D-VA) and Rep. Ed Markey (D-MA). The bill would require all commercial e-mail messages to be identified as such (but not with a standard label, except for sexually explicit messages), and to include the sender's physical street address and an opt-out mechanism; messages relating to a specific transaction and consented to by the recipient would be exempt from those requirements. The bill would prohibit commercial e-mail messages with false or misleading message headers or misleading subject lines, and it would be illegal to send commercial e-mail messages to addresses generated by an automated dictionary attack. State laws that restrict the sending of commercial e-mail, regulate opt-out procedures, or require subject-line labels would be pre-empted; laws that merely regulate falsification of message headers would remain in effect.

Ban on Deceptive Unsolicited Bulk Electronic Mail Act of 2003 (S. 1052)

The Ban on Deceptive Unsolicited Bulk Electronic Mail Act of 2003 was introduced by Sen. Bill Nelson (D-FL) in May 2003. It would prohibit the inclusion of false information in message headers in unsolicited bulk commercial e-mail. It also would require senders of unsolicited bulk commercial e-mail to include opt-out instructions and honor opt-out requests, and would prohibit them from harvesting e-mail addresses of potential recipients from web pages and other sources. Violations of the law could be prosecuted under RICO.

CAN-SPAM Act of 2003 (S. 877)

The Controlling the Assault of Non-Solicited Pornography and Marketing Act was reintroduced by Senators Conrad R. Burns (R-MT) and Ron Wyden (D-OR) in April 2003, with only minor changes from the previous year's version, S. 630 (2002). The CAN-SPAM Act of 2003 would require unsolicited commercial e-mail messages to be labeled (though not necessarily by a standard method) and to include opt-out instructions and the sender's physical address. The law would prohibit the use of deceptive subject lines and false headers in such messages. It would pre-empt any state laws that prohibit unsolicited commercial e-mail outright, but would not affect the majority of state spam laws. The bill was amended in committee in June 2003, but the amended text is not yet available.

Computer Owners' Bill of Rights (S. 563)

The Computer Owners' Bill of Rights, introduced by Sen. Mark Dayton (D-MN) in March 2003, would require the Federal Trade Commission to establish a "do-not-email" registry of addresses of persons and entities who do not wish to receive unsolicited commercial e-mail messages. The FTC would be empowered to impose civil penalties upon those who send unsolicited commercial e-mail to addresses listed on the registry.

Criminal Spam Act of 2003 (S. 1293)

The Criminal Spam Act of 2003 was introduced on June 19, 2003, by Sen. Orrin Hatch (R-UT); among the co-sponsors are several senators who have sponsored other bills listed here. The bill would prohibit unauthorized or deceptive use of a third party's computer for relaying bulk commercial e-mail messages. It also prohibits the use of false header information in bulk commercial messages, and regulates the use of multiple e-mail accounts or domain names for purposes of sending such messages. The law would apply only to quantities of more than 100 messages within 24 hours, or 1000 within 30 days, or 10,000 within one year.

REDUCE Spam Act of 2003 (H.R. 1933)

The Restrict and Eliminate the Delivery of Unsolicited Commercial Electronic Mail or Spam Act of 2003 was introduced by Rep. Zoe Lofgren (D-CA) in May 2003. Under the REDUCE Spam Act, unsolicited bulk commercial e-mail messages would be required to include a valid reply address and opt-out instructions, and a label ("ADV:" or "ADV:ADLT", or other recognized standard identification). These requirements would apply to messages sent in the same or similar form to 1,000 or more e-mail addresses within a two-day period. In addition, false or misleading headers and deceptive subject lines would be prohibited in all unsolicited commercial e-mail messages, whether or not sent in bulk.

Reduction in Distribution of Spam Act of 2003 (H.R. 2214)

The Reduction in Distribution of Spam Act of 2003 was introduced in May 2003 by Rep. Richard Burr, R-NC; cosponsors include Energy and Commerce Committee chairman Rep. Billy Tauzin, R-LA, and Judiciary Committee chairman Rep. James Sensenbrenner, R-WI. The bill would require all commercial e-mail messages to be identified as such (but not with a standard label, except for unsolicited sexually explicit messages), and to include the sender's physical address and an opt-out mechanism. It would prohibit the use of false or misleading headers in commercial messages. State laws that prohibit unsolicited commercial e-mail, regulate opt-out procedures, or require subject-line labels would be pre-empted; laws that merely regulate falsification of message headers would remain in effect.

Stop Pornography and Abusive Marketing Act (S. 1231)

Sen. Charles Schumer (D-NY) introduced the Stop Pornography and Abusive Marketing Act, or "SPAM Act," in June 2003. The bill would establish a national "no-spam" registry, and make it unlawful to send unsolicited commercial messages to addresses on that list. The list would be administered by the FTC, using fees paid by marketers for access to the list. The FTC would be empowered to prohibit explicit commercial messages to minors even if they were not on the list. All unsolicited commercial messages would be required to use a label ("ADV:") at the beginning of the subject line, except those sent in compliance with an FTC-approved self-regulatory program. It would be illegal to send any commercial e-mail in violation of an Internet service provider's policies, or with a false or misleading subject line or message header, or to harvested addresses; all commercial messages would be required to include the sender's physical address.

Wireless Telephone Spam Protection Act (H.R. 122)

H.R. 122, introduced by Rep Rush D. Holt (D-NJ) in January 2003, would prohibit the use of wireless messaging systems to send unsolicited advertisements.

Appendix D – State Laws Regulating SPAM[64]

Alaska: Alaska enacted a law in May 2003 that requires a label ("ADV:ADLT") at the beginning of the subject line of any sexually explicit unsolicited commercial e-mail message, if the sender knows that the recipient is an Alaska resident.

Arizona: An Arizona law enacted in May 2003 requires that unsolicited commercial e-mail messages include a label ("ADV:") at the beginning of the subject line, and contain an opt-out mechanism. Such messages may not contain falsified routing information. The law prohibits false or misleading subject lines in all commercial e-mail, and prohibits the use of a third party's Internet address or domain name without consent in order to make it appear that the third party sent the message. The law applies if a message is sent from within Arizona, or if the recipient's service provider is based in or has equipment in Arizona, or if the sender knows or has reason to know that the recipient is an Arizona resident.

Arkansas: Under Arkansas laws enacted in April 2001 and April 2003, all commercial and sexually explicit e-mail messages must include a functioning reply e-mail address and opt-out instructions; opt-out requests must be honored. Unsolicited sexually explicit messages must also contain a label ("ADV:ADULT") at the beginning of the subject line. In addition, unsolicited commercial and sexually explicit messages must include the sender's name, physical address, and domain name, and may not use a third party's domain name without permission, nor misrepresent the point of origin or routing information. It is illegal to distribute software designed to falsify routing information.

California: Under legislation approved in September 1998, unsolicited commercial e-mail messages must include opt-out instructions and contact information, and opt-out requests must be honored. Certain messages must contain a label ("ADV:" or "ADV:ADLT") at the beginning of the subject line. A provider may sue a sender of unsolicited commercial e-mail for violating the provider's policies if the sender has actual notice of such policies. The law applies to e-mail that is delivered to a California resident via a provider's facilities located in California.

Colorado: The Colorado Junk Email Law, enacted in June 2000, prohibits the sending of unsolicited commercial e-mail that uses a third party's Internet address or domain name without permission, or contains false or missing routing information. Unsolicited commercial e-mail messages must contain a label ("ADV:") at the beginning of the subject line, and must include the sender's e-mail address and opt-out instructions; opt-out requests must be honored. The law applies to e-mail that is sent to Colorado residents via a provider's service or equipment located in Colorado.

Connecticut: A Connecticut law enacted in June 1999 makes it illegal to send unsolicited bulk e-mail containing falsified routing information in violation of a provider's policies, or to distribute software designed to falsify routing information. A court may exercise personal jurisdiction over a nonresident who uses a computer or computer network located in Connecticut.

Delaware: Under legislation approved in July 1999, it is illegal to send unsolicited bulk commercial e-mail, to send unsolicited bulk e-mail containing falsified routing information, or to distribute software designed to falsify routing information. The law applies to messages originating outside the state if the recipient is located in Delaware and the sender is aware of facts making the recipient's presence in Delaware a reasonable possibility.

Idaho: A law approved in April 2000 requires that unsolicited bulk commercial e-mail messages must include an e-mail address for opt-out requests and requires senders to honor opt-out requests. Such messages may not

64 The summaries of state laws regulating SPAM are listed at the SPAM.LAWS website. The following is cited in accordance with the terms and conditions of reference: David E. Sorkin, Spam Laws, http://www.spamlaws.com/. <http://www.spamlaws.com/state/summary.html>, visited 7/10/2003.

use a third party's name for the return address without permission, and must contain accurate routing information.

Illinois: Legislation approved in July 1999 makes it illegal to send an unsolicited commercial e-mail message using a third party's domain name without permission; containing falsified routing information; or with a false or misleading subject line. The law applies to e-mail that is delivered to an Illinois resident via a provider's facilities located in Illinois. A separate provision makes it illegal to send unsolicited bulk e-mail with falsified routing information or to distribute software designed to falsify routing information.

Indiana: An Indiana law approved in April 2003 prohibits commercial e-mail that uses a third party's domain name without permission, includes a false or misleading subject line, or misrepresents its point of origin or other routing information. Unsolicited commercial e-mail messages must include a label ("ADV:" or "ADV:ADLT") at the beginning of the subject line, along with opt-out instructions. The law applies to messages sent from outside Indiana if the sender knows that the recipient is an Indiana resident, or if that information is available upon request from the registrant of the domain name contained in the recipient's e-mail address.

Iowa: An Iowa law approved in May 1999 prohibits the sending of unsolicited bulk e-mail that uses a third party's name for the return address without permission, or contains false or missing routing information. Unsolicited bulk commercial e-mail messages must include opt-out instructions and contact information, and opt-out requests must be honored. The law applies to e-mail that is sent to or through a computer network located in Iowa.

Kansas: Under a Kansas law enacted in May 2002, commercial e-mail messages may not contain falsified routing information, use a third party's domain name without permission, or have a false or misleading subject line. Senders of commercial e-mail messages must include opt-out instructions and honor opt-out requests. Unsolicited bulk commercial e-mail messages (500 or more recipients) and advertisements for sexually explicit content must contain a label ("ADV:" or "ADV:ADLT") at the beginning of the subject line. The law applies if a message is sent from within Kansas, or if the sender knows that the recipient is a Kansas resident. The law also prohibits the distribution of software designed to falsify routing information.

Louisiana: A Louisiana law approved in July 1999 makes it illegal to send unsolicited bulk commercial e-mail to more than 1,000 recipients if the e-mail messages contain falsified routing information or the sender uses a provider's facilities to transmit the messages in violation of the provider's policies. The law also prohibits the distribution of software designed to falsify routing information. Louisiana's obscenity law was amended in June 2003 to cover electronic communications. Commercial e-mail messages with sexually explicit content must include a label ("ADV-ADULT") at the beginning of the subject line.

Maine: Maine enacted legislation in May 2003 that requires unsolicited commercial e-mail to contain a label ("ADV:" or "ADV:ADLT") at the beginning of the subject line, and include the sender's name and valid e-mail address and opt-out instructions; opt-out requests must be honored. Such messages may not use a third party's Internet address or domain name without permission, nor contain falsified routing information. The law applies to messages sent to two or more recipients within the state.

Maryland: Under a Maryland law enacted in May 2002, it is illegal to send a commercial e-mail message that uses a third party's domain name without permission; that contains false or missing routing information; or with a false or misleading subject line. The law applies if a message is sent from within Maryland; if the sender knows that the recipient is a Maryland resident; or if the registrant of the domain name contained in the recipient's address will confirm upon request that the recipient is a Maryland resident.

Minnesota: A Minnesota law enacted in May 2002 prohibits commercial e-mail that uses a third party's domain name without permission, contains false routing information; or has a false or misleading subject line. Such messages must contain opt-out instructions and contact information. Unsolicited commercial e-mail messages must contain a label ("ADV:" or "ADV-ADULT") at the beginning of the subject line. The law applies to messages sent to Minnesota residents through facilities located in Minnesota.

Missouri: A Missouri law enacted in June 2000 requires unsolicited commercial e-mail messages to contain opt-out instructions and contact information.

Nevada: In July 1997 Nevada became the first state to enact spam legislation. As amended in 2001 and 2003, Nevada law provides that it is illegal to send unsolicited commercial e-mail unless it is labeled "ADV" or "ADVERTISEMENT" at the beginning of the subject line, and includes the sender's name, street address, and e-mail address, along with opt-out instructions. Nevada law prohibits all unsolicited e-mail that contains falsified routing information; that is sent with the intent to disrupt the normal operation or use of a computer, Internet site, or e-mail address; or that is reasonably likely to cause such disruption. The state also prohibits the distribution of software that is designed to falsify routing information.

New Mexico: New Mexico enacted legislation in April 2003 requiring that unsolicited commercial e-mail messages contain a label ("ADV:" or "ADV:ADLT") at the beginning of the subject line, and opt-out instructions at the top of the message body.

North Carolina: Legislation approved in June 1999 makes it illegal to send unsolicited bulk commercial e-mail containing falsified routing information, if the sender thereby violates a provider's policies. The law applies to e-mail sent into or within the state.

North Dakota: A North Dakota law enacted in April 2003 prohibits the sending of unsolicited commercial e-mail messages that contain a false or misleading subject line, use a third party's domain name without permission, or misrepresent the point of origin or routing information. All commercial e-mail messages must include an opt-out mechanism. In addition, unsolicited commercial messages must contain a label ("ADV" or "ADV-ADULT") at the beginning of the subject line. The law applies to messages sent from outside the state if the sender knows that the recipient is a North Dakota resident, or if that information is available upon request from the registrant of the domain name contained in the recipient's e-mail address.

Ohio: An Ohio law approved in August 2002 requires unsolicited commercial e-mail messages to contain the sender's name, address, and e-mail address, along with opt-out instructions, and requires senders to honor out-out requests; these requirements do not apply to messages sent based upon a "direct referral" from another person. It is illegal to forge the sender's address or other routing information in commercial e-mail messages. The law also enables a provider to sue a sender of commercial e-mail for violating the provider's policies if (1) the sender had actual notice of such policies, or (2) the policies were posted on the provider's web site and were communicated electronically to the sender's computer.

Oklahoma: An Oklahoma law approved in June 1999 and amended in April 2003 makes it illegal to send an e-mail message that contains false or missing routing information, or to distribute software designed to falsify such information. Unsolicited commercial e-mail messages must include a label ("ADV:" or "ADV-ADULT:") at the beginning of the subject line, and must contain opt-out instructions. Such messages may not contain a false or misleading subject line, nor use a third party's Internet address or domain name in order to make it appear that the third party sent the message. A court may exercise personal jurisdiction over a nonresident who sends a message to or through the network of a provider located in Oklahoma.

Pennsylvania: Under Pennsylvania laws approved in June 2000 and December 2002, unsolicited commercial e-mail may not use a third party's domain name without permission or include a false or misleading subject line, and must include a valid reply address and an opt-out mechanism. Sexually explicit unsolicited commercial e-mail must contain a label ("ADV-ADULT") at the beginning of the subject line. In addition, falsification of routing information in unsolicited e-mail is unlawful, as is the distribution of software designed to facilitate falsification of routing information.

Rhode Island: Under legislation approved in July 1999, it is illegal to send unsolicited bulk e-mail with falsified routing information using a Rhode Island provider in violation of the provider's policies, or to distribute software designed to falsify routing information. A separate law requires unsolicited commercial e-mail messages to include opt-out instructions and contact information, and opt-out requests must be honored; it is illegal to send unsolicited commercial e-mail using a third party's domain name without permission or containing false routing information. This law applies to messages sent from a computer located in Rhode Island and to messages sent into the state, if the sender had reason to know that the recipient was a Rhode Island resident or the recipient had previously submitted an opt-out request to the sender.

South Dakota: Legislation approved in February 2002 prohibits sending commercial e-mail that misrepresents or obscures its point of origin or routing information, or contains a false or misleading subject line. The law applies if a message is sent from within South Dakota; if the sender knows that the recipient is a South Dakota resident; or if the registrant of the domain name contained in the recipient's address will confirm upon request that the recipient is a South Dakota resident. Unsolicited commercial e-mail messages must contain a label ("ADV:" or "ADV:ADLT") at the beginning of the subject line.

Tennessee: Under legislation approved in June 1999, unsolicited bulk commercial e-mail messages must include opt-out instructions and contact information, and opt-out requests must be honored. Certain messages must contain a label ("ADV:" or "ADV:ADLT") at the beginning of the subject line. The law applies to e-mail that is delivered to a Tennessee resident via a provider's facilities located in Tennessee. The distribution of software designed to falsify routing information is also prohibited. (Use "without authority" is defined to include sending unsolicited bulk e-mail in violation of a provider's policies, although the statute does not provide any consequences for such use.)

Texas: Texas enacted legislation in June 2003 requiring that unsolicited commercial e-mail messages include a label ("ADV:" or "ADV: ADULT ADVERTISEMENT") at the beginning of the subject line, and a functioning return e-mail address for opt-out requests, which must be honored. The law prohibits unsolicited commercial messages with falsified routing information. False, deceptive, or misleading subject lines are prohibited in all commercial e-mail messages, as is the unauthorized use of a third party's domain name.

Utah: Legislation enacted in March 2002 applies to unsolicited commercial e-mail and unsolicited sexually explicit e-mail that is sent through a provider in Utah or to a resident of Utah. Such messages must disclose the sender's name and physical address, and the point of origin of the message; and must include a label ("ADV:" or "ADV:ADULT") at the beginning of the subject line, along with opt-out instructions. The law also prohibits the falsification of routing information in such messages.

Virginia: Legislation approved in March 1999 makes it illegal to send unsolicited bulk e-mail containing falsified routing information, if the sender thereby violates a provider's policies, or to distribute software designed to falsify routing information. A court may exercise personal jurisdiction over a nonresident who uses a computer or computer network located in Virginia. The law was amended in April 2003 to increase the penalties for sending a high volume of messages containing falsified routing information.

Washington: Under a Washington state law enacted in March 1998 and amended in May 1999, it is illegal to send a commercial e-mail message that uses a third party's domain name without permission; that contains false or missing routing information; or with a false or misleading subject line. The law applies if a message is sent from within Washington; if the sender knows that the recipient is a Washington resident; or if the registrant of the domain name contained in the recipient's address will confirm upon request that the recipient is a Washington resident.

West Virginia: A law enacted in March of 1999 makes it illegal to send unsolicited bulk e-mail messages in violation of a provider's policies that use a third party's domain name without permission, misrepresent the point of origin or other routing information, have a false or misleading subject line, or contain sexually explicit materials. Each message must include the sender's name and return e-mail address, along with the date and time it was sent. It is also illegal to distribute software designed to falsify routing information. The law applies if a message is sent from a computer located in West Virginia, or if the sender knows or has reason to know that the recipient is a resident of West Virginia.

Wisconsin: In June 2001 Wisconsin enacted a statute that requires unsolicited commercial e-mail messages that contain obscene material or depict sexually explicit conduct to include the words "ADULT ADVERTISEMENT" in the subject line. A separate Wisconsin statute prohibits e-mail harassment (Wis. Stat. § 947.0125), but does not appear to apply to most unsolicited bulk or commercial e-mail.

Wyoming: A Wyoming law approved in March 2003 (effective July 1, 2003) prohibits commercial e-mail that uses a third party's domain name without permission, includes a false or misleading subject line, or misrepresents its point of origin or other routing information. It is unlawful to assist in the transmission of such messages, which apparently includes operating an open relay. The law applies to messages sent from outside Wyoming if the sender knows that the recipient is a resident of Wyoming or a jurisdiction with a similar law, or if that information is available upon request from the registrant of the domain name contained in the recipient's e-mail address.