15th BILETA Conference: "ELECTRONIC DATASETS AND ACCESS TO LEGAL INFORMATION".

Friday 14th April 2000.
University of Warwick, Coventry, England.

Regulating Spams on the Internet

Wye-Keen Khong
Cyberlaw Centre, Faculty of Management
Multimedia University
Cyberjaya, Malaysia

ABSTRACT

This paper briefly surveys the movement to regulate spams or unsolicited commercial emails on the Internet. It discusses the history of spam, definition of spam, and identifies parties fighting spam. Also, it examines legislative efforts to regulate spam and the various schemes and mechanisms employed.

KEYWORDS

Spam; Unsolicited Commercial Email; Unsolicited Bulk Email.

A BRIEF HISTORY OF SPAM

Spam is a US trade mark for a canned meat product from Hormel Foods. In Internet lingo, `spam' refers to the mass mailing of unsolicited advertisement through electronic means.

The Net Abuse FAQ (*Southwick & Falk,* 1998) provides a fairly detailed description of the origin of this word. The word `spam' is commonly ascribed to a skit performed on the British television show Month Python's Flying Circus, in which the word `spam' is repeated to the point of absurdity in a restaurant menu (*CompuServe Inc. v. Cyber Promotions, Inc. and Sanford Wallace,* 1997). Its usage on the Internet is rumoured to have originated from the MUD/MUSH community where one of the users assigned a keyboard macro to the line "SPAM SPAM SPAM SPAM SPAM SPAM SPAM SPAM SPAM SPAM SPAM SPAM SPAM SPAM SPAM" and proceeded to send it to the MUD once every couple of second (*Southwick & Falk,* 1998). This incident apparently ingrained in the memory of the MUD users and the act was known as `spamming'.

A spam therefore is the multiple posting of the same message, and spamming is the act thereof. Spams generally appear in two places: emails and newsgroups. An email spam happens when the same message is sent to multiple recipients.

Initially, a distinction was made between newsgroups spam and cross-posting. Newsgroups spamming entails sending an identical copy of the message to every newsgroup, while cross-posting referred to sending a single copy of the message, but addressing it to several different newsgroups (Loundy, 1995). Technically speaking, cross-posting to newsgroups is not spam, because only one copy of the same message resides in every news server (*Southwick & Falk,* 1998). Most news reader

programs are intelligent enough to indicate that a cross-posted message has been read in another newsgroup while the same programs will treat spammed messages in newsgroups as separate unread ones.

Because delivery of emails uses a different protocol from that of news, the ways to combat spams on these platforms are also different. Technically it is easier to remove spams on newsgroup through the use of cancelbot and other intelligent agents (*Southwick & Falk,* 1998). Conversely, because of the nature of the mail transport protocol which does not require authentication, email spams are difficult to control, and hence receives more attention from the courts and legislatures. In this paper, the focus of the discussion will be on email spams.

WHO IS AGAINST SPAMS?

Spams are objected by two groups of people: email users and network administrators. Email users object to spams for the reason that they incur unnecessary cost and time when dealing with undesirable emails in their mailbox. For users who pay for connection time to the Internet, downloading an additional email which is later found to be useless or a nuisance means money wasted. Even if the user gets his Internet connection free or for a flat fee, he still wastes time sifting through his emails, separating junk from genuine. Also, if there is too much spam, the mailbox may overflow and prevent legitimate emails from entering. Email users generally categorise this as a cost-shifting exercise. Because the cost of sending bulk emails, minus the cost to the users, is far too low compared to its success rate, spammers and Internet marketer are in favour of legalising spams instead of banning them (Eccles, 1999).

The practice of sending huge amount of emails to the Internet poses a more serious problem to network administrators. In the first place, a deluge of emails to a mail server may severely cripple the network of an Internet service provider (ISP). According to a report by an Internet security firm, 14% of Internet email is spam or bulk emails (Wareham, 1999). Netcom, an ISP, reports that spam increases the cost of support by 15% to 20%, administration by 20%, incoming delivery by 10%, disk space by 15%, and overall equipment cost of 10% to 15% (Dern, 1998). In addition, 5% to 30% of the 14 million emails going to American Online daily are spam (Dern, 1998). The effect of these spams on ISPs are network outages and congestions, and the increasing demand for faster and bigger bandwidth to satisfy the same number of users.

Apart from the increased cost of running a network, ISPs have to bear the brunt of users' complaints when they receive spams in their mailboxes. Some frustrated customers threatened to close their accounts unless the ISPs do something to reduce the amount of spam. Hence, spam potentially affects the business opportunity of ISPs and forces network administrators to actively filter spams on their servers.

The third damage done by spams to network administrators is the loss of reputation. Many a times, spammers forge false return email addresses belonging to an ISP, and when angry email users return or bounce the spam, they end up at the ISPs' servers. Unsuspecting Internet users will think that it was the ISPs or network administrators who sanctioned the spams. In addition, severe network outage could result when this email fraud is being carried out.

It can be seen that the basis of objections by email users and network administrators are quite different. Email users object to spams because of their content, while network administrators disapprove because of the quantity or bulk.

DEFINING SPAM

Even though users' objection differs from network administrators', the solution for both appears to be simply ban spam or the bulk sending of emails. Assuming this step is taken, certain questions have to

be considered before such a law is made.

First, what is the basis of such a ban? Under tort law, not all nuisances are actionable. For a nuisance to be actionable, it must be done under negligent or subject to strict liability. Emails and the Internet are such new things that the court has yet to decide whether emails can be subject of nuisance law. Consider this: one difference between emails and other objects of nuisance is that emails become annoying when `there is too much of a good thing'. Since by having an email address impliedly mean the willingness to receive emails, it is difficult to conceptualise the turning point when emails become objectionable. One possible exception to this dilemma is when the user gives explicit notice to a sender that he does not wish to receive further emails from him, and failing to heed the notice gives rise to an action under nuisance law.

Some countries such as the United States have constitutional protection for free speech which raises the question of the extent laws can be enacted to ban spams (Carroll, 1996; Byrne, 1998). In the United States, the degree of constitutional protection for political speech is different from commercial speech. Commercial speech gets less protection and can be regulated by law provided the law fulfils certain conditions (*Central Hudson Gas and Electric Corporation v. Public Service Commission of New York,* 1980). For this reason, the movement to have laws regulating spams only cover `unsolicited commercial emails' as against `bulk emails'.

The difference between `unsolicited commercial emails' and `bulk emails' is succinctly described by Coalition Against Unsolicited Bulk Email, Australia [Caube.au] (n.d.1). Basically it boils down to the inability of U.S. legislatures to regulate communication which may potentially conflict with political free speech protection. In countries where this limitation is less likely to happen, regulating bulk emails makes better sense than confining to commercial emails.

Also, another issue is the definition of `commercial'. Different states and countries may have different interpretation of this word. This may give rise to the problem of over-legislate at one hand, and under-legislate at the other. For example, many services nowadays, such as education, require payment of a fee, and equally many or more websites offer free services to its customers and potential customers. The California Assembly Bill 1676 of 1998 describes `commercial' as "advertising material for the lease, sale, rental, gift offer, or other disposition of any realty, goods, services, or extension of credit", which is rather comprehensive.

There is a third kind of spam known as acquaintance spam. The Coalition Against Unsolicited Bulk Email, Australia [Caube.au] (n.d.1) explains acquaintance spam as "spam that is sent to you by somebody you have dealt with previously". Acquaintance spam may be problematic in legislating for two reasons. First, many a times, spams from acquaintance are sent in good faith and under the impression that the emails are useful or of interest to the recipients, therefore are more targeted than many of the commercial spams. Secondly, because of prior dealings or contact, the recipient might have implicitly or explicitly consented to the spams. Nevertheless acquaintance spam is still spam, and will take up the network bandwidth, and network administrators will still complain if the load is too much. An extension to acquaintance spam is referral spam. That mean, a spam sent by a website through a referral by an acquaintance Many websites which provides incentive to their users for successful referrals have strict policies against referral spams. That means the users are encouraged to submit referrals, but are prohibited from flooding the system with every email addresses that they can get their hands on.

The first problem in regulating spam is to define spam. As discussed, this is not a simple problem. Different interpretations have different implications. The utopian definition of spam will net all email communications which are of no benefit to the recipient, from the recipient's point of view, and exclude all those which are beneficial from the same recipient's point of view.

THE FIGHT AGAINST SPAM

In the early days of the Internet, social behaviour on the Internet is governed by a form of custom, affectionately known as `netiquette' (see Hambridge, 1995). The source of this `netiquette' or network etiquette is mostly from network administrators' acceptable use policies (see Mueller & Panitz, n.d.). These acceptable use policies serve as agreements between the network administrators and their users on what are and are not acceptable practises when using the Internet. The policies in turn are influence by the technical limitations of the Internet protocols. This is to make the Internet function effectively (Hambridge & Lunde, 1999).

Through time, these acceptable usage policies became a custom of the Internet. Network administrators formed consensus and follow standards. Internet users were presumed to have consented to these netiquettes upon going onto the Net. Any apparent breach was to arouse the ire of other users. Sanctions of various kind, from reprimands to denials of access, were imposed on the offending parties. Sometimes, the network administrator of these offending parties was also rebuked for his inability to solicit proper behaviour from his users. This vigilante or frontier justice (Loundy, 1995) has the effect of compelling new users to take note of the existing netiquette. Commentators suggest that this netiquette has the weight of customary law (Carroll, 1996).

When the Internet was transformed from an academic and research network into a commercial concern (Zakon, 2000), the scene changed. More non-technical users started to use the Internet blissfully ignorant of the netiquettes. At the same time, commercialisation and advertisements started to appear as part of Internet services. This was also the time when Internet users became more open to commercial content on the Internet. And from then on, commercial spammers start to operate.

One of the first and most notorious spam was inflicted by the US attorney couple Lawrence Canter and Martha Siegel. One day in 1993, they sent out identical "green card" advertisements to every newsgroup they can find. They received many prospective leads. But they also found themselves at the receiving end of more angered users. Some users retaliated by relaying multiple emails to them, causing massive overloading of their mailbox and their network provider's server. Other irate hackers tried to knock down the server by hacking it. One ingenious hacker created a `cancelbot' to automatically wipe out every copy of the offensive message in the newsgroups.

The Canter and Siegel episode demonstrates clearly that there was some kind of rule in force. There was no court, no arbiter, and no prosecutor. Instead, users took the `law' into their own hands. Collectively, the sanction imposed could be enormous. This is an evidence of `mob law' or `vigilante regulation'.

In time, spammers became wiser. They forged email headers, used unsuspecting public email relay servers, and provided false return addresses. This caused further difficulties to the Internet community, particularly the network administrators. Many an instance servers owning the forged domains were forced to the point of shut down, swamped by bounce emails and unintentional returning hate mails.

Since the first spam, network administrators and Internet users have been devising various technical methods to overcome this problem of spams. Some include filtering mails going to the email accounts, blocking spam emails from an entire server, blocking Usenet newsgroup spam for an enter server, and blocking IP connectivity from spam sites.

One Internet service provider is billing spammers for the resources they used (R&D Associates, 1998). Their argument is that it is for the "time required in training [their clients] and cleaning [the] servers, and the space that was used in storing [the spammers'] documents." However, so far, they were still far from being successful in their claim.

On the legal side, some Internet service providers (ISPs) have taken spammers to court based on a few causes of action. From the ISP's point of view, sending unsolicited commercial emails to the

ISP's server after repeated request and warning to stop doing so is a trespass to property (*CompuServe Inc. v. Cyber Promotions, Inc. and Sanford Wallace,* 1997). This argument has been upheld in the court. Others reasons for action includes the spammers breaching the agreement with their Internet service provider for sending spam. Also, their spams cause Internet users' retaliation, which shut down the ISP's server. Further, the forged false headers and return addresses cause innocent businesses network outage and loss of reputation. Action under trade mark infringement and false trade description may also be possible. Spamming is considered an unacceptable activity by the US courts, and the courts have allowed injunctions against spammers to send unsolicited commercial emails to specific sites. More recently, a Canadian court has recognised spamming as against netiquette, which further strengthens ISP's position against spammers (*1267623 Ontario, Inc. v. Nexx Online Inc.,* 1999).

LEGISLATING SPAM

On the legislative front, some efforts have been made by the federal and state legislatures of the United States and some European countries. Countries which have not enacted any law on spamming are examining this issue since it is a global problem and not confined to within a jurisdiction. Overall, different approaches have been taken in regulating spams. These approaches or legal mechanisms are described further below.

The most vocal group in promoting a ban against spams is the Coalition Against Unsolicited Commercial Email [CAUCE] (n.d.1) and their affiliated counterparts in other countries, i.e. European Coalition Against Unsolicited Commercial Email [EuroCauce] (n.d.1), Coalition Against Unsolicited Bulk Email, Australia (n.d.2), and Coalition Against Unsolicited Commercial Email, India (n.d.).

At the time of writing, 14 states in the U.S. have enacted laws relating to spams (Geller, 1999; Sorkin, 2000). They are California, Connecticut, Delaware, Illinois, Iowa, Louisiana, Nevada, North Carolina, Oklahoma, Rhode Island, Tennessee, Virginia, Washington, and West Virginia. State legislation started with Nevada (1997). This was followed by Washington, California and Virginia. The laws passed by these four states subsequently became models for the other ten states (Geller, 1999).

Law-making at the federal level has not been as successful. Various bills were presented at the senate and house of representatives by the pro and anti-spam proponents. However, none has yet to pass into law. The first approach to tackling spam at the U.S. federal level is to examine the language of Telephone Consumer Protection Act of 1991, 47 U.S.C. § 227. The Telephone Consumer Protection Act prohibits, *inter alia,* "the use of any telephone facsimile machine, computer, or other device to send an unsolicited advertisement to a telephone facsimile machine". Through the Act's overbroad definition of a "telephone facsimile machine", it is possible to cover unsolicited advertisement emails (Sorkin, 1997).

In 1997, CAUCE proposes an amendment to the Telephone Consumer Protection Act to explicitly cover unsolicited commercial emails. This proposed amendment was taken up by Repulican representative in the House of Representative Christopher Smith. On 21 March 1997, he presented his Netizens Protection Act of 1997 to the House. With the amendment, not only are spams outlawed, Internet users who are spammed get a private right of action to sue the spammer US$500 for each message. If the court believes that the spammer wilfully or knowingly violated the law, the claims are tripled. However this amendment has died in the 105th Congress.

On the same day as Smith's Bill, Senator Frank Murkowski presented a bill to regulate spam. This Unsolicited Commercial Electronic Mail Choice Act of 1997 was vigorously supported by spammers, but strongly opposed by CAUCE. This bill seeks to legalise spamming as long as it fulfil certain formalities, such as the word "Advertisement" appears first in an email's subject line, "the

name, physical address, electronic mail address, and telephone number of the person who initiates transmission of the message", and valid Internet routing information. The biggest drawback of the bill is that it imposes a legal obligation upon ISP to install filtering mechanisms on their server, to publicise the availability of this feature, and to actively help users to filter spams if they seek so.

The latest in the pipeline is the Unsolicited Electronic Mail Act of 1999 (H.R. 3113). This bill seeks to incorporate the best parts of earlier bills, such as the requirement of a valid return email address, forces spammers to honour opt-out requests, outlaws forged headers, empowers ISPs to bring spammers to court for violating of access policies, allows ISPs to collect payment for sending spams to their users, allows ISPs to implement spam filters, allows individuals and corporations to use spammers in civil court, authorises the Federal Trade Commission to pursue violation of law, and finally, provides for an exception where the sender and the recipient have an existing business relationship but retains the right to rescind permission by the recipient. By far, this is the most comprehensive of all, although it still falls short of what most advocates want--banning all but opt-in schemes.

On the international front, several countries have amended their laws to regulate spams. Article 10 of the European Union Distance Selling Directive (European Parliament and Council, 1997) prohibits automatic machine communication without prior consent of the consumer. This has been interpreted to cover unsolicited commercial emails.

At the time of writing, Austria, Denmark, Finland, Germany and Italy have laws to regulate commercial or unsolicited emails (Caube.au, n.d.3). Austrian law requires the prior revocable consent of the recipient (EuroCauce, n.d.2). In Denmark, unsolicited emails are prohibited (EuroCauce, n.d.3). In Finland, sending of unsolicited commercial emails to private person and newsgroups is unlawful (EuroCauce, n.d.4). In Germany prior consent is required for all contacts (EuroCauce, n.d.5), but in Italy, this is only confined to emails for advertising purposes (EuroCauce, n.d.6).

REGULATORY MECHANISMS

A couple of different regulatory mechanisms have been devised by legislature and proponents as evidenced from the bills they tabled. These mechanisms include the requirement for valid identification in the email, provision for out-out scheme, clean-up damages for ISPs, identifier in subject line to aid filtering tools, SMTP banner notification, revocable opt-in scheme, and outright ban.

Valid Identification

Because of technical backlash from angered spam recipients, many spammers do not use valid email addresses and email headers in their spams. More advanced spammers use special programs to send spam with spoofed headers. Spoofing is the introduction of false or inaccurate headers in emails in order to fool servers and users into thinking that the emails came from a certain location. The danger of spoofing is that it may cause harm to an innocent network administrator when his server becomes the target of bounced emails and mail bomb attacks.

The California Assembly Bill 1676 (1998) requires a "valid sender operated return e-mail address". Delaware, Louisiana, North Carolina, Oklahoma, Rhode Island, Virginia, Washington and West Virginia presently have laws prohibiting address forgery or false headers in emails (Geller, 1999).

Opt-Out Schemes

The requirement of a valid return email address is tied closely to the implementation of opt-out schemes. An opt-out scheme gives a spammer the right to send spams to recipients unless the

recipients email or sign up a form to inform the spammer that they do not wish to continue receiving spams from him. This is the mechanism most favoured and championed by the Direct Marketing Association (Eccles, 1999).

Opt-out scheme was first introduced in the direct mail industry as a response for a call to regulate commercial mails (Sovern, 1999). The Direct Marketing Association has extended the idea to spams by introducing an e-Mail Preference Service (Direct Marketing Association, n.d.). The e-Map Preference Service works by allowing a spammer to send his list of email addresses to the service and let the service "clean up" addresses which have been registered. What proponents of opt-out scheme fail to see is that this system can be easily abused.

The opt-out scheme is criticised for various reasons. First there is no proof that spammers will honour an opt-out scheme. In fact, it has been shown that spammers are not members of the traditional direct marketing organisations, which understands the value of self-regulation. Many spams are one time spam from advertisers. If every potential advertisers send one spam each, much time and effort would have to be wasted to opt out. Even if the spam recipient sends an email or filling in a web-based form to opt-out, it will be taken as a sign that the email is valid and alive. The effect is that the email address is more valuable and more spams will ensue. Similarly, a simple computer program may be used to compare the source and output of the e-Mail Preference Service to single out those addresses that have been removed. These addresses would be more valuable because the addresses are alive and valid, and that the recipients have taken an active effort to register themselves with the service. This will also cause more spams to the addressese. Studies have shown that the longer an email account is being used, the more spams it will receive (Riggs, 1999). One reason could be that the addresses are sold to the spammers.

Although opt-out scheme is the one most disfavoured by anti-spam advocates, legislature frequently is pressured by the direct marketing industry to introduce a compromise. California, Delaware, and Rhode Island have laws to provide for opt-out scheme (Geller, 1999).

Clean-Up Damages

Damages is a good deterrent against spams. Many of the laws provide statutory damages to individuals and ISPs. These damages vary from US$10 per message in Colorado and Iowa to US$500 in Rhode Island. Besides, some states also allow recovery of actual clean up costs to the network administrators.

Identifier in Subject Line

One other control mechanism that has been suggested is to use email filters. Although this does not at all reduce the amount of spam, it helps recipients filter unwanted emails. To enable this filtering mechanism to work more efficiently, a specific keyword has to be place in the email header. The best place to do so is at the subject line of the emails. The California Act for example, requires all unsolicited commercial email to have the words "ADV:" at the beginning of the subject line, and "ADV: ADLT" if the spam contains adult advertisement (Geller, 1999). Since there is only one subject line in each email, to make this system work, all laws implementing the mechanism must use the same keywords. Hence, Colorado's law requires the same implementation as California's.

SMTP Banner Notification

This is another technological innovation to control spams. Legal recognition of a "no-spam" SMTP banner will pave the way for the enforcement of anti-spam policy based on technology (Cauce, n.d.2). The SMTP banner notification allows the network administrator of a mail server to configure its server to send a "no-spam" message to any servers requesting permission to send emails. This shortcuts the need for human intervention and notification before sending spams become a trespass.

The Can Spam Act (H.R. 2162, 1999) introduced by Rep. Garry Miller of California contains a provision for recognition of SMTP banner notification.

Revocable Opt-In Scheme

By far, opt-in scheme is the most favoured by anti-spam advocates. Opting in means that the recipient has actively given prior consent to send commercial emails to him. The advantage of opt-in scheme is that it reduces the number of spams on the Internet, and recipient could not complain since they have given consent. To make opt-in scheme work, it must be the only mechanism allowed by law. When the recipient no longer wishes to recipient the emails, a corresponding opt-out method must be provided by the advertisers. Unlike United States, many European countries have adopted opt-in scheme as the only lawful way of sending commercial emails.

Outright Ban

The pristine view that the Internet should be free from all commercial activities has long gone since the National Science Foundation has relinquished its control over the Internet backbone in 1995 (Zakon, 2000). Although some countries such as Denmark and Italy have laws which prevent direct marketing, the general consensus is that an outright ban would be inconceivable to the growth of the Internet. As stated, the more preferred mechanism is to ban unsolicited commercial emails and legalise opt-in solutions.

CONCLUSION

This paper is a preliminary study of the movement to regulate spams on the Internet. There is still no global consensus as to the proper regulatory mechanism. Further, the issue of transborder spamming activities are yet to be adequately resolved, further studies and discussion have to be conducted. As email addresses are not an indication of the recipients' physical location, it would be technically impossible to prevent a commercial email from reaching a recipient in a country which outlaws spam. Like many of the cyberlaw issues, an agreed global protocol would have achieved many milestones in the fight against spams on the Internet.

REFERENCES

Byrne, Jonathan. (1998, February 14). Squeezing spam off the net: Federal regulation of unsolicited commercial e-mail. *West Virginia Journal of Law & Technology, 2(1).* Available: http://www.wvjolt.wvu.edu/v2i1/byrne.html.

Carroll, Michael W. (1996, Fall). Garbage in: Emerging media and regulation of unsolicited commercial solicitations. *Berkeley Technology Law Journal, 11(2).* Available: http://www.law.berkeley.edu/journals/btlj/articles/11_2/Carroll/html/reader.html.

Coalition Against Unsolicited Commercial Email. (n.d.1). *Welcome to CAUCE.* Available: http://www.cauce.org/.

Coalition Against Unsolicited Commercial Email. (n.d.2). *SMTP banner notification proposal.* Available: http://www.cauce.org/proposal/index.shtml.

Coalition Against Unsolicited Commercial Email, India. (n.d.).*Welcome to CAUCE India.* Available: http://www.india.cauce.org/.

Coalition Against Unsolicited Bulk Email, Australia. (n.d.1).*What is spam?* Available: http://www.caube.org.au/whatis.htm.

Coalition Against Unsolicited Bulk Email, Australia. (n.d.2).*Fight spam in Australia.* Available: http://www.caube.org.au/.

Coalition Against Unsolicited Bulk Email, Australia. (n.d.3).*National laws overseas.* Available: http://www.caube.org.au/natlaws.htm.

Dern, Daniel P. (1998, May 4). Postage due on junk e-mail: Spam costs Internet millions every month. *InternetWeek, 713.* Available: http://www.techweb.com/se/directlink.cgi?INW19980504S0003.

Direct Marketing Association. (n.d.). *e-Mail preference service.* Available: http://www.e-mps.org/en/.

Eccles, Matthew. (1999, May 20). Opt-out system is the right way to tackle spam. *Marketing Week,* p. 42. Available: ProQuest ABI/Inform.

European Coalition Against Unsolicited Commercial Email. (n.d.1).*EuroCAUCE homepage.* Available: http://www.euro.cauce.org/en/.

European Coalition Against Unsolicited Commercial Email. (n.d.2).*Austria.* Available: http://www.euro.cauce.org/en/countries/c_at.html.

European Coalition Against Unsolicited Commercial Email. (n.d.3).*Denmark.* Available: http://www.euro.cauce.org/en/countries/c_dk.html.

European Coalition Against Unsolicited Commercial Email. (n.d.4).*Finland.* Available: http://www.euro.cauce.org/en/countries/c_fi.html.

European Coalition Against Unsolicited Commercial Email. (n.d.5).*Germany.* Available: http://www.euro.cauce.org/en/countries/c_de.html.

European Coalition Against Unsolicited Commercial Email. (n.d.6).*Italy.* Available: http://www.euro.cauce.org/en/countries/c_it.html.

Geller, Tom. (1999, December). State law update. *Cauce News 3(4).* Available: http://www.cauce.org/newsletter/v3n4.shtml.

Hambridge, S. (1995, October). Netiquette guidelines. (IETF RUN Network Working Group, RFC 1855). Available: http://www.ietf.org/rfc/rfc1855.txt.

Hambridge, S., & Lunde, A. (1999, June). Don't spew: A set of guidelines for mass unsolicited mailings and postings (spam*). (IETF RUN Network Working Group, RFC 2635). Available: http://www.ietf.org/rfc/rfc2635.txt.

Loundy, David. (1995, March 9). Lawyers' electronic ads leave bad taste. *Chicago Daily Law Bulletin,* p. 6. Available: http://www.Loundy.com/CDLB/Spam.html.

Mueller, Scott Hazen, & Panitz, Aliza R. (n.d.). *Sample acceptable use policies.* Available: http://spam.abuse.net/spam/aup.html.

Netizens Protection Bill, H.R. 1748, 105 Cong. (1997).

R&D Associates. (1998). *History of a dispute with a spammer.* Available:

http://www.kclink.com/spam/.

Riggs, Brian. (1999, June 7). After a while, it all looks like spam. *Information Week,* p.14. Available: ProQuest ABI/Inform.

Sorkin, David E. (1997, Fall). Unsolicited commercial e-mail and the Telephone Consumer Protection Act of 1991. *Buffalo Law Review, 45,* 1001-1032. Available: Lexis.

Sorkin, David E. (2000). *Spam laws: United States: State laws: Summary.* Available: http://www.spamlaws.com/state/summary.html.

Southwick, Scott, & Falk, J.D. (1998). *The net abuse FAQ.* Available: http://www.cybernothing.org/faqs/net-abuse-faq.html.

Sovern, Jeff. (1999, October). Opting in, opting out, or no options at all: The fight to control of personal information. *Washington Law Review, 74,* 1033-1188. Available: Lexis.

Wareham, Elynn. (1999, May 14). Spam and e-mail abuses costing millions: Survey. *Computing Canada,* 25(19), 1.

Zakon, Robert Hobbes. (2000). *Hobbes' Internet timeline v5.0.* Available: http://info.isoc.org/guest/zakon/Internet/History/HIT.html.

CASES CITED

1267612 Ontario, Inc. v. Nexx Online Inc., [1999] O.J. No. 2246 (Court file no. C20546/99). Available: http://legal.web.aol.com/decisions/dljunk/nexxorder.html.

CompuServe Inc. v. Cyber Promotions, Inc. and Sanford Wallace, 962 F. Supp. 1015 (S.D. Ohio Feb 3, 1997).

Central Hudson Gas and Electric Corporation v. Public Service Commission of New York, 447 U.S. 557 (1980).

STATUTES CITED

California Assembly Bill 1676 of 1998, § 17538.4. Available: http://www.jmls.edu/cyber/statutes/email/cal1676-2.html.

European Parliament and Council. (1997, 20 May). Directive on the protection of consumers in respect of distance contracts, 97/7/EC. Available: http://europea.eu.int/comm/dg24/policy/developments/dist_sell/dist01_en.html.

Nevada Senate Bill 13 of 1997, § 41.705-735.

Available http://www.suespammers.org/nv/41-705-735.shtml.