BUSTING BLOCKS: APPROPRIATE LEGAL REMEDIES FOR WRONGFUL INCLUSION IN SPAM FILTERS UNDER U.S. LAW

Jonathan I. Ezor
Assistant Professor and Director, Institute for Business, Law and Technology,
Touro College Jacob D. Fuchsberg Law Center, Central Islip, NY.

This paper discusses the growth and increasing significance of e-mail in the business and personal environment, and how unsolicited bulk commercial e-mail, also known as spam, has become a significant drain on technical and economic resources. It analyzes the statutory and self-help efforts to combat spam, focusing on block lists and automated spam filters, and how alleged spammers have brought lawsuits in U.S. courts claiming they had been wrongfully included within block lists and filters. Finally, it describes possible claims under U.S. law, then argues for a higher standard of care among block list vendors and the need for recourse to courts when self-help remedies for mistaken block listing fail.

Introduction: A Short History of Spam

Commercial use of the Internet was restricted by the Acceptable Use Policy of the National Science Foundation until March 1991.[1] With the lifting of that restriction, the full commercial exploitation of the Internet, including electronic mail,[2] began in full force, including the spread of unsolicited bulk commercial messages, which quickly gained the nickname "spam."[3] Although the first spam e-mail reportedly occurred as early as 1978[4] and the first widely-reported spam occurred in 1994 not e-mail but on Usenet,[5] e-mail spam began to build serious momentum in the late 1990s. As the percentage of spam as a total of each user's e-mails grew, service providers, software vendors and the legal system were pressured to reduce the burden.

Initially, spam recipients and their Internet service providers ("ISPs") seeking legal redress and injunctive relief were limited to adapting existing offline doctrines such as "trespass to chattels" to the unauthorized use of their servers and computers as bulk e-mail conduits. While some cases, particularly those brought by ISPs, were successful,[6] others, such as Intel v. Hamidi,[7] found United States courts less than willing to extend this doctrine to e-mail.

The Rise of Anti-Spam Legislation

Eventually, legislatures took up the effort against spam, first in individual states[8] and then in Congress with the federal CAN-SPAM Act.[9] The statutes largely focused on labeling advertisements, prohibiting misleading techniques (such as disguising the sender's identity or disregarding unsubscribe requests by unwilling recipients), and requiring proper identification of the senders (such as postal addresses).[10] Even this approach poses problems, since an e-mail message may include both advertising and informational material. How should a law characterize a newsletter which includes legitimate articles separated by sponsor advertisements? The advertisements themselves may be unsolicited, and the volume of the newsletter might lend itself to a definition of "bulk," but the overall publication may not qualify as "spam".

Another major hurdle faced by anti-spam legislation is enforcement. Any statute must address jurisdiction (interstate and international), both to bring the alleged spammer into court and to enforce penalties. Before establishing jurisdiction, though, the enforcement agency or litigant must identify the spammer. This is not a simple process. The Internet enables both anonymity[11] and pseudonymity,[12] and a major tactic of spammers is to falsify the sending information of the message, making it even difficult to determine the actual sender. Spammers also frequently change ISPs and accounts,[13] and even when they are found, they may have hidden their assets.[14] Even where spamming is made a felony, as in Virginia,[15] convictions are rare.

Block Lists and Spam Filters: Self-Regulation Through Technology

Before legislators began fighting spam, though, the Internet's users were addressing it using two methods: block listing and filtering. Block listing began as a way to name (and therefore shame) the most egregious spammers, with Paul Vixie's "Real-time Blackhole List" being the first such resource.[16] Vixie's block list was implemented on a user level and sender-by-sender basis. As e-mail usage migrated to the consumer level, and as spam became more of a problem, the Internet community began scaling up efforts to block spam. The "block list" evolved into a downloadable, standardized tool for ISP mail server computers, blocking all e-mail from senders the list designated as spammers. These lists were maintained largely by volunteers, including The Spamhaus Project ("Spamhaus")[17] in the U.K., while others, such as Julian Haight's SpamCop,[18] began as volunteer efforts but were later acquired by commercial firms. Vendors such as Symantec[19] offered software incorporating block lists as well.

Block lists populate their databases of spammers in a number of ways. List managers create unused e-mail "trolling" accounts on popular ISPs. Spammers using "dictionary attacks," in which they send bulk commercial messages to every possible combination of numbers and letters making up possible e-mail addresses, will unknowingly include the trolling accounts. Once the account receives a commercial message (by definition unsolicited, since the list managers never provide the troll address to anyone), its details are added to the block list.

Another method focuses on the servers through which spam is sent. E-mail server computers may be configured to reject messages coming through them from outside their network or pass the outside messages along to their destinations. Those that pass along messages indiscriminately are called "open mail relays," and are frequently utilized by spammers to disguise the spam's origin.[20] Given this risk, spam opponents have sought to discourage open relays by creating public open relay block lists[21], as well as other lists of similar exploits.[22] Even where a server is not open to the public, where its authorized users send spam through it, the server (and all of its users, spammer and non-spammer alike) may get added to block lists. This possibility is of particular importance to those Internet Service Providers who may offer connectivity services to company networks as well as individuals. The ISPs disable connecting mail servers (whether spammer or corporate) to their network in order to prevent the ISP from being deemed "spammer friendly," but that can inconvenience legitimate high-volume mailers and corporate customers.

Collaborative reporting is a third method for populating block lists. In this model, users report spam to list owners.[23] Depending on how the block list operates, the information may be immediately added to the block list or investigated further.

In parallel with the rise of shared block lists, e-mail programs themselves offer internal spam filters as a feature for users. Microsoft's Outlook e-mail program, for example, based its blocking on a combination of suspect terms and user feedback.[24]

As spammers have become more sophisticated at modifying their messages (including falsifying sender information) to beat simpler blocking methods, software-based filters have incorporated heuristic methodologies, analyzing words, punctuation, sender information, mail server information, and other elements to score incoming messages as spam (called Bayesian[25] filtering), based on work by the 18th century theoretician Rev. Thomas Bayes.[26]

Spam(mer) Labeling and the Challenge of False Positives

The processes by which messages are filtered as "spam" are not perfect. Definitions of objectionable spam vary. One definition provides that

> "[a]n electronic message is "spam" IF: (1) the recipient's personal identity and context are irrelevant because the message is equally applicable to many other potential recipients; AND (2) the recipient has not verifiably granted deliberate, explicit, and still-revocable permission for it to be sent; AND (3) the transmission and reception of the message appears to the recipient to give a disproportionate benefit to the sender."[27]

To the Interactive Advertising Bureau, spam is "unsolicited email that can fill up your inbox with nuisance advertisements or scams."[28] The Direct Marketing Association merely provides guidelines on responsible e-mail marketing[29], while laws may either define spam directly[30] or list prohibited activities with regard to electronic mail[31]. Each user has her own idea of what constitutes "junk" e-mail.[32]

Even when no one has directly identified a message as spam, an automated filter operating on pre-existing rules and methods may improperly tag a non-commercial or solicited message as spam. This could happen because of the use of an

open relay, because of the incorporation of elements within the message which are also common to spam, because a previous spammer falsely used that sender's address as its own, or because some combination of characteristics adds up to a filter trigger.

Unfortunately, however the message is kept from its intended destination, the sender may never know it hasn't arrived, because filtered spam may be automatically deleted or redirected to an spam or junk mail folder. At times, a sender may only determine it has been added to a block list because of a lack of response to the sent message. In this way, even local false positives can remain problems, particularly if the sender's identity rather than the message contents cause the blocking. If the false positive happens on a multi-network basis, detection and remediation may be much more difficult. Worse still, some block lists may even go beyond the actual sender of the message, listing companies that have apparently benefited from or facilitated the spam.[33]

The Potential Impact of False Positives and Wrongful Labeling

For a casual e-mail exchange, a blocked message or account can be inconvenient. On the other hand, a false positive in a spam filter or block list can make the difference between winning a bid for a government contract[34] or not, cause a litigant to miss a court-imposed deadline where pleadings are to be sent via e-mail,[35] or otherwise cost time, money or both.

In the commercial context, the risks can be both harder to quantify and greater in scope. Even the most zealous anti-spam advocates acknowledge that a solicited commercial message may be proper. Definitions of solicitation, however, may vary. Spamhaus, for example, states that a message is solicited when "the recipient has…verifiably granted deliberate, explicit, and still-revocable permission for it to be sent."[36] In sharp contrast, the Direct Marketing Association's "E-mail Delivery Best Practices" provide a much broader view on solicitation, including both opt-in and opt-out.[37]

False positives, though, can keep even a solicited message from reaching not only a single recipient but millions of recipients, if the false positive is generated by a block list shared across users or ISPs.[38] This is not just a hypothetical situation for direct marketers. The Interactive Advertising Bureau has published an entire guide to e-mail deliverability,[39] which states, "More than 20% of legitimate marketing messages are incorrectly identified as spam by server and client level spam filtering…."[40] Given that the IAB's members are among the larger and more-established (and therefore legally exposed) marketers[41], it is likely that the processes by which these companies obtain and utilize lists are more detailed and conservative than those used by more aggressive, smaller marketers.

Remedying Improper Listing: The Limits of the Self-Regulatory Approach

Within the Internet's tradition of collaborative self-regulation,[42] senders can try to remedy false labeling without an outside arbiter (i.e. a court). To address false

positives from filters run by individual recipients, many senders include explicit instructions[43] for the recipients to add the sender to a "white list," a list of approved e-mailers. [44] This requires an affirmative act by the user, and given the number of different software and ISP combinations through which users receive e-mail,[45] mailers may find this approach less than successful.[46] It also applies only to single e-mail accounts.

A more scalable approach involves getting on the white list of the larger ISPs. While this is more efficient than relying upon individual white lists, it still requires a multi-step process for each ISP. Not every ISP maintains a global white list, however; some leave the process in the hands of users.[47] Those senders that do not send commercial bulk e-mail may not even pursue white listing before being blocked. In either event, the white listing process is imperfect, and companies may still end up on block lists and spam filters by mistake or through the malice of critics or competitors.

Another approach is to obtain third-party certification as a non-spammer.[48] The requirements are detailed,[49] and the applicability, though widespread,[50] is far from universal. For many e-mailers, the costs or efforts of compliance may be too great.

The most efficient approach is to request removal directly from the particular block list. The first significant challenge is discovering the listing; while some vendors such as Spamhaus make their lists public, others do not.[51] A mail sender on a closed list may only suspect it is there by examining which ISPs seem to be blocking its mail. This method may not be determinative, especially if the ISPs use multiple lists and filters for most complete coverage.[52]

Even where a sender knows on which filter(s) it has been placed, removal is far from certain. Some vendors have published processes for removal;[53] others may not. The sender may also face a presumption of invalidity. [54] Some lists will not even accept proposed evidence from accused spammers; the accused's ISPs must argue on its behalf. If an ISP is unwilling or unable to assist, the accused may face the choice of remaining on the block list or switching ISPs (which can itself raise suspicion among anti-spam advocates).

Because of the severe potential consequences of having one's e-mail blocked, many accused spammers retain attorneys to advocate on their behalf with the block lists. Block list owners may believe that any sender utilizing an attorney is an actual spammer using unfounded legal threats to coerce removal.[55] No matter the circumstances, though, a vendor may elect not to remove the sender from its lists.

Litigation as a Remedy: Existing Cases and Evolving Doctrine

If a sender believes itself to be wrongfully included on a block list and is unable to obtain removal after exhausting all self-help processes and remedies, what can it do? Under U.S. law, e-mail senders may be able to look to the courts for redress, requesting equitable relief, monetary damages, or both.

Existing Spam Filter Litigation in U.S. Courts

There have been a number of reported cases in U.S. courts regarding wrongful operation of spam filters. Some have focused on free speech rights under the

First Amendment to the U.S. Constitution.[56] Others have turned in part on a unique U.S. law: 47 U.S.C. §230. This statute, passed in response to cases such as Stratton Oakmont v. Prodigy,[57] is expressly meant to encourage the growth of the Internet.[58] Section (c) of §230 states,

> (1) Treatment of publisher or speaker
> No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.
> (2) Civil liability
> No provider or user of an interactive computer service shall be held liable on account of--
> **(A)** any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected; or
> **(B)** any action taken to enable or make available to information content providers or others the technical means to restrict access to material described in paragraph (1).

Section e(3) goes on to state in relevant part that "no cause of action may be brought and no liability may be imposed under any State or local law that is inconsistent with this section."

The Black Ice and OptInRealBig Cases: Exploring the Limits of 47 U.S.C. §230

A number of defendants in spam filter cases have raised 47 U.S.C. § 230 as a defense. One significant example is Mail Abuse Prevention System LLC v. Black Ice Software.[59] In Black Ice, Mail Abuse Prevention System ("MAPS"), a vendor of spam filter services, listed Black Ice as a spammer in its "Realtime Blackhole List," then sued under California's anti-spam law.[60] In response, Black Ice cross-complained, accusing MAPS of "(1) defamation; (2) intentional interference with contractual relationship; (3) intentional interference with prospective economic advantage; (4) unfair competition; and (5) restraint of trade." [61] After rejecting MAPS' motion for summary judgment, the court turned to the counterclaims.

MAPS raised 47 USC §230 as a complete defense. The court found MAPS had standing under (c)(2) of §230 as an "access software provider" since it "enable[d] other computer users accessing the Internet." The court then analyzed whether spam would be considered "harassing" or "otherwise objectionable" content under (c)(2). While the court accepted that spam could fall into that definition, MAPS had also blocked other messages and servers beyond the alleged objectionable spam, so Black Ice's counterclaims were allowed to be further adjudicated.

The defamation claim was based on MAPS' calling Black Ice a spammer, a statement for which Black Ice did not have to plead actual damages under California defamation law.[62] According to the court's analysis of Section (c)(2)(B) of §230, MAPS' listing of Black Ice as a spammer was not merely a technical enabling of spam blocking but an "announcement" which was a separate act. Accordingly, the

defamation claim was allowed to stand. While the claim of intentional interference with contractual relations was rejected, the other claims (intentional interference with prospective economic advantage, unfair competition and restraint of trade) were permitted to stand, as was Black Ice's claim for punitive damages. In addition to the Black Ice case (for which no further opinions were disseminated), MAPS was also involved in litigation with other firms including Media3,[63] Yesmail,[64] Exactis (later Experian),[65] and Harris Interactive.[66]

The Black Ice case contrasts sharply with another reported opinion, OptInRealBig.com v. Ironport Systems[67]. In that case, the plaintiff, a direct e-mail marketer, sued Ironport over the reporting by Ironport subsidiary Spamcop.net of OptInRealBig as a spammer to OptInRealBig's ISPs. Unlike MAPS, Spamcop functioned by passing along complaints from recipients of alleged spam to the sender's ISP. Given that Spamcop was passing along others' reports of spam in accordance with the definition of 47 U.S.C. §230,[68] the court found that the statute fully protected Spamcop/Ironport. Even after upholding Ironport's immunity under §230, though, the court went on to analyze and reject OptInRealBig's claims regarding trade libel, interference with contractual relations, and unfair business practices.[69]

e360 v. Spamhaus: Jurisdictional Issues in International Block Lists

The most recent case to be reported regarding block lists involves e360 Insight ("e360") and the Spamhaus ROKSO (Register of Known Spam Operations)[70] list. According to the papers and histories for the case made available by e360[71] and Spamhaus[72] and the electronic case records of the Northern District of Illinois,[73] e360 (located in Wheeling, Illinois) brought first brought suit in June 2006 in the Illinois Circuit Court (a state court) against Spamhaus (based in the UK), alleging that Spamhaus had improperly listed e360 on the ROKSO list even though e360 denied having been a spammer or otherwise qualifying for the ROKSO list. After e360 obtained a temporary restraining order, Spamhaus requested (and received) removal of the case to the U.S. District Court for the Northern District of Illinois. Spamhaus then denied that the court had jurisdiction over it,[74] after which Spamhaus' attorneys withdrew from the case.[75] On September 13, 2006, Judge Kocoras of the District Court entered a default judgment against Spamhaus for $11,715,000 in damages and $1,971.05 in litigation costs. After e360 requested that the court order ICANN[76] to suspend the Spamhaus.org domain name as part of its proposed remedies, new attorneys appeared for Spamhaus, and Spamhaus gave notice that it intended to appeal the default judgment. Ultimately Judge Kocoras denied the suspension of the domain name,[77] and the action was still pending as of late October 2006.

While e360's claims are similar to those in the Black Ice and OptInRealBig cases, the jurisdictional dispute and default nature of the judgment makes it difficult to analyze the strength of e360's arguments. The case, though, raises the question of whether an out-of-state (or offshore) entity that knowingly incorporates a company into a spam filter should be held responsible for damages caused in the jurisdiction of the listed company. This question has been examined in the online context in other U.S. cases including Bochan v. La Fontaine[78] and U.S. v. Ivanov[79], and internationally against a U.S.-based Web publisher in Australian courts for alleged defamation of an

Australian citizen.[80] Should e360 prevail on the jurisdictional question, it could open the door for U.S. lawsuits against Spamhaus and other international block list providers.

Wrongful Inclusion in Block Lists or Filters: The Elements of Potential Claims

In a situation in which a party believes it has been wrongfully included in a spam filter or block list and therefore has been damaged, what type of claims are likely to succeed in U.S. courts? While the answer (and controlling precedents) will vary among jurisdictions, the strongest arguments are likely to cover defamation and intentional interference with prospective business relationships.

The below analysis presupposes that the sender added to the block list in fact is not a spammer under a definition accepted by the court hearing the case. If the sender is in fact a spammer, its ability to make the below claims, particularly with regard to defamation, can be substantially impaired. The other assumption is that the block list vendor is not able to take advantage of 47 USC §230 because it does not fit into one of the categories provided in the statute (e.g. interactive service provider; transmitting information provided by a third party; etc.).[81]

Defamation

As has been shown in this article, spamming is not only viewed by the Internet community as negative activity[82] but is a crime in a number of jurisdictions.[83] These facts lay the foundation for a defamation action. According to the Restatement (Second) of Torts:

> "To create liability for defamation there must be:
> (a) a false and defamatory statement concerning another;
> (b) an unprivileged publication to a third party;
> (c) fault amounting at least to negligence on the part of the publisher; and
> (d) either actionability of the statement irrespective of special harm or the existence of special harm caused by the publication." [84]

This applies to businesses as well as individuals:

> One who publishes defamatory matter concerning a corporation is subject to liability to it
> (a) if the corporation is one for profit, and the matter tends to prejudice it in the conduct of its business or to deter others from dealing with it, or
> (b) if, although not for profit, it depends upon financial support from the public, and the matter tends to interfere with its activities by prejudicing it in public estimation.[85]

Publishing an accusation of a crime which can result in imprisonment[86] or a statement which damages the subject's ability to do its business is actionable per se without need to show special damages.[87] Accordingly, in a situation where a sender is wrongfully identified as a spammer to potential service providers and customers, and the block list vendor has done so either negligently or maliciously, the sender may

have an action in defamation. Even where a block list is not itself made public, the blocking process may be sufficient to indicate that a particular sender has been designated as a spammer.

Intentional Interference with Prospective Business Relationships

Another possible claim is the tort of intentional interference with prospective contractual relation:

> One who intentionally and improperly interferes with another's prospective contractual relation (except a contract to marry) is subject to liability to the other for the pecuniary harm resulting from loss of the benefits of the relation, whether the interference consists of
> (a) inducing or otherwise causing a third person not to enter into or continue the prospective relation or
> (b) preventing the other from acquiring or continuing the prospective relation.[88]

While this tort has been adopted by a number of states, its required elements differ.[89] In situations where alleged spammers are publicly identified on block lists, the clear intention is to keep the sender from doing business. This is even more demonstrable where not only bulk messages but all messages from the sender or even the sender's Web site are blocked, impeding the sender's ability to operate at all.[90]

Other Possible Claims

Depending on the facts of the case and applicable law, other claims that may be brought include but are not limited to unfair competition, restraint of trade, and interference with contractual relations. The blocked party may also be able to demonstrate actual damages, to the extent that a blocked communication caused specific harm.

Conclusion: Balancing the Equities and Setting the Standards

Spam places a real time and financial burden on networks and users, and the incentives of e-mail as a marketing tool (minimal cost, easy automation, worldwide reach) encourage new spammers to enter the field. At the same time, there can be significant harm to innocent senders caught improperly in spam filters, given that the most popular block lists and filters control entry into the inboxes of millions of users across numerous ISPs. To what standard, then, should filter vendors be held?

One could argue that market forces will be sufficient to keep block lists under control and acting responsibly. If a block list generates too many false positives, users will reject it for a more accurate product. On a macro level, this makes sense, but it helps little at the margins, where a single legitimate mailer's messages (or even Web site) are blocked. Unless the sender's messages are missed by large numbers of users, the impact of an incorrect blocking of that sender on the community as a whole will be minimal and any resulting market forces pushing toward better lists negligible.

For the sender, though, the consequences can be severe, and without the ability to use the courts to force a change, the sender may have little recourse.

If, on the other hand, courts hold block list and filter vendors accountable for their failure to properly police their lists for false positives, and exercise jurisdiction even over an offshore block list, block list vendors may have to take notice. To reduce the likelihood of court action, block list vendors should evolve the definitions of spamming they use toward objective standards rather than the opinions they are based on today.[91] Additionally, complaining senders should be automatically delisted absent objective proof of repeated violations. Further, block list providers should limit their blocking to the actual IP address used to send the alleged spam rather than taking it upon themselves to block the e-mail or even Web site of the perceived beneficiary of the message (i.e. the party whose products are being advertised).[92]

The bottom line is that even the volunteer block list providers are knowingly and intentionally affecting numerous commercial relationships and the financial health of companies. They should therefore be held to professional standards of conduct, including objectivity, reasonable care, and (to the extent their activities cause harm) accountability. The alternative, relying on their good faith and internal procedures, is no longer acceptable, given how critical e-mail has become. Just as letter carriers are held accountable when, due to their actions, mail is neither delivered nor returned,[93] because of the importance of what can be contained in postal mail, block list and spam filter vendors (who may not directly deliver the e-mail, but knowingly interpose their services in the process for their users) must make every reasonable effort to ensure that they are not keeping legitimate e-mail from its destination, or face the consequences of their lack of care.

---

[1] NSFNet, National Science Foundation Network. Retrieved November 4, 2006 from http://www.livinginternet.com/i/ii_nsfnet.htm.

[2] Bekker, Scott (2005, Jan. 18). Study: 651 Million E-mail Users Worldwide. *Redmondmag.com*. Retrieved November 4, 2006 from http://redmondmag.com/news/article.asp?EditorialsID=6527.

[3]The term "spam" itself comes from a 1970 Monty Python's Flying Circus sketch. Ford, Roger Allan (2005). Preemption Of State Spam Laws By The Federal CAN-SPAM Act, *University of Chicago Law Review, 72*, 355 n.1.

[4] http://www.templetons.com/brad/spamreact.html.

[5] Moody, Glyn (2004, March 5). Spam's Tenth Birthday Today. Retrieved November 4, 2006 from http://news.netcraft.com/archives/2004/03/05/spams_tenth_birthday_today.html.

[6] See, e.g., Compuserve v. Cyber Promotions, Inc., 962 F.Supp. 1015 (S.D.Ohio,1997).

[7] 30 Cal.4th 1342 (2003) (former employee not prohibited from sending thousands of critical e-mail messages into employer's e-mail system).

[8] See, e.g., Sorkin, David. Spam Laws: Summary. Retrieved November 4, 2006, from http://www.spamlaws.com/state/summary.shtml (state-by-state summary of current spam laws).

[9] Controlling The Assault Of Non-Solicited Pornography And Marketing Act Of 2003, PL 108-187 (December 16, 2003).

[10] CAN-SPAM, note 9 supra.
[11] See, e.g., http://www.anonymizer.com/consumer/products/anonymous_surfing/; http://tor.eff.org/ (anonymous Internet communications system funded by Electronic Frontier Foundation, an online rights advocacy group).
[12] "Pseudonymity is the use of pseudonyms as IDs." Tu Dresden, Department Of Computer Science, Institute For System Architecture (2004, July 22). Anonymity, Unobservability, Pseudonymity, and Identity Management – A Proposal for Terminology. Retrieved November 4, 2006, from dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.18.pdf.
[13] Roberts, Paul (2003, May 7). EarthLink Wins $16 Million in Spam Case. *IDG News Service*. Retrieved November 4, 2006, from http://pcworld.com/article/id,110627-page,1/article.html) (describes how convicted spammer Howard Carmack was pursued by EarthLink, which "shut down several accounts he used.").
[14] See, e.g., Levenson, Michael (2006, August 17). In Dispute With Spammer, AOL Hunts Gold. *Boston Globe.* Retrieved November 4, 2006, from http://www.boston.com/news/local/articles/2006/08/17/in_dispute_with_spammer_aol_hunts_gold/.
[15] Va. Code Ann. § 18.2-152.3:1 (defines spamming as a misdemeanor and, if transmission or revenue exceeds certain levels, a class 6 felony).
[16] See, e.g., McMillan, Robert (1997, December). What Will Stop Spam. *SunWorld*. Retrieved November 4, 2006, from http://sunsite.uakom.sk/sunworldonline/swol-12-1997/swol-12-vixie.html (interview with Paul Vixie about RBL).
[17] http://www.spamhaus.org.
[18] http://www.spamcop.net.
[19] *Symantec Brightmail AntiSpam*. Retrieved October 23, 2006, from http://eval.veritas.com/mktginfo/enterprise/fact_sheets/ent-factsheet_brightmail_antispam_6.0_08-2004.en-us.pdf.
[20] See, e.g., Neubauer, Joseph (2002, June 21). Fortify Your Email Transport – Part 2. Retrieved October 13, 2006, from http://www.microsoft.com/technet/prodtechnol/exchange/2000/deploy/frtfytr2.mspx.
[21] See, e.g., ORDB, the Open Relay Database (http://www.ordb.org);
[22] See, e.g., NJABL (Not Another Just Bogus List) (http://www.njabl.org); the Spamhaus XBL (Exploits Block List) (http://www.spamhaus.org/XBL/).
[23] See, e.g., Cloudmark Desktop. Retrieved November 4, 2006, from http://www.cloudmark.com/desktop.
[24] *OL98: How to Filter Junk and Adult Content E-Mail*. Retrieved November 4, 2006, from http://support.microsoft.com/?kbid=182251.
[25] See, e.g., Paul Graham, "A Plan for Spam," http://www.paulgraham.com/spam.html.
[26] Bayes, Rev. Thomas (1763). An Essay Towards Solving A Problem In The Doctrine Of Chances. Retrieved November 4, 2006, from http://www.stat.ucla.edu/history/essay.pdf.
[27] *MAPS' Definition of Spam.* Retrieved October 13, 2006, from http://www.mail-abuse.com/spam_def.html.

[28] *Internet Advisory Board – Definition of Terms.* Retrieved October 13, 2006, from http://www.iab.ie/FAQs/DefinitionofTerms/.
[29] Direct Marketing Association (2005, October). Council For Responsible E-Mail, E-Mail Delivery Best Practices For Marketers And List Owners. Retrieved October 13, 2006, from http://www.the-dma.org/antispam/EmailBPFINAL.pdf.
[30] The State of Illinois defines spam as "unsolicited electronic mail advertisements", 30 ILCS 500/25-70.
[31] See, e.g., CAN-SPAM Act, note 9, supra.
[32] See, e.g., Vogt, Carlton (2001, April 6). Spam: The Name's the Same, But We're Still Not Sure What It Means. *Infoworld*. Retrieved October 13, 2006, from http://www.itworld.com/Man/2695/IWD010406opethics/.
[33] See, e.g., Gaudin, Sharon and Gaspar, Suzanne (2001, September 10). The Spam Police. *NetworkWorld.* Retrieved November 4, 2006, from http://www.networkworld.com/research/2001/0910feat.html (Mail Abuse Prevention System listed iBill as a spammer and blocked its 254 IP addresses when one of iBill's customers allegedly spammed a customer).
[34] See, e.g., Instructions for Electronic Bid Submissions, Grayson County, TX. Retrieved October 13, 2006, from http://www.co.grayson.tx.us/Purchasing/PurchaseBidSub.htm; See also Delaware State Budget, Fiscal, Procurement and Contracting Regulations, § 6902(9), 29 Del.C. § 6902.
[35] As of October 2006, the New York State Court of Claims is operating a pilot Filing by Electronic Means ("FBEM") program. The Attorney General's office has established a procedure for being served via e-mail as part of that process. Office of the Attorney General of the State of New York, Service on the Attorney General by E-mail. Retrieved October 13, 2006, from http://www.oag.state.ny.us/serviceag/serviceag.html.
[36] http://www.spamhaus.org/definition.html (accessed on October 19, 2006).
[37] http://www.the-dma.org/antispam/EmailBPFINAL.pdf (accessed October 13, 2006).
[38] "Brightmail AntiSpam solutions are used to filter over 15 percent of worldwide email and over 100 billion emails per month." Symantec, *Symantec Brightmail AntiSpam*. Retrieved October 19, 2006, from http://www.symantec.com/Products/enterprise?c=prodinfo&refId=835. As of September 2006, the user base for the Spamhaus Block List "exceeded 621,829,000 internet users." *Spamhaus SBL Frequently Asked Questions*. Retrieved October 13, 2006 from http://www.spamhaus.org/faq/answers.lasso?section=Spamhaus%20SBL#7.
[39] Interactive Advertising Bureau (2006). *Marketer & Agency Guide to Email Deliverability*. Retrieved October 19, 2006, from http://www.iab.net/emaildeliverability.
[40] Id. at p. 3.
[41] Interactive Advertising Bureau (2006). *IAB About*. Retrieved on November 5, 2006, from http://www.iab.net/about/general_members.asp.
[42] See, e.g., Dibbell, Julian (1998). *A Rape in Cyberspace*. Retrieved November 5, 2006, from http://www.juliandibbell.com/texts/bungle.html.

[43] "If you use spam filters to protect your in-box, please take a moment right now to add newsletter@guidestar.org to your e-mail address book, spam software white list, or mail system white list. Adding the address will help ensure that you receive the Newsletter and that your e-mail software displays HTML and images properly." Guidestar.org (August 2006). *Guidestar Newsletter*.
[44] The Computer Language Company (2006). *Tech Encyclopedia: White List*. Retrieved November 5, 2006, from http://www.techweb.com/encyclopedia/defineterm.jhtml?term=whitelist.
[45] See, e.g., PromoSuite Interactive (2005, September 15). *How to Make Sure Listeners Receive Your Email*. Retrieved October 19, 2006, from http://www.listeneremail.com/email/emailhelp.htm.
[46] McDonald, Loren (2005, October 26). *How to Get on a White List*. Retrieved October 19, 2006, from http://www.emaillabs.com/email_marketing_articles/email_marketing_isp_relations_whitelists.html.
[47] EarthLink's spamBlocker provides for individual rather than ISP-wide white lists. *EarthLink spamBlocker for Windows Users*. Retrieved October 19, 2006, from http://www.earthlink.net/software/free/spamblocker/bulk/#allow.
[48] See, e.g., Sender Score Certified, http://www.senderscorecertified.com.
[49] Return Path, Inc. (2006). *Email Standards*. Retrieved November 5, 2006, from http://www.senderscorecertified.com/standards.html.
[50] "Sender Score Certified is the industry's leading accreditation system, used by more than 35,000 receiving domains…covering more than 250 million email mailboxes worldwide." Return Path, Inc. (2006, April 18). *Return Path Re-Launches the Bonded Sender Program with More Rigorous Standards and New Name, Sender Score Certified*. Retrieved November 5, 2006, from http://www.returnpath.biz/resources/archives/2006/04/return_path_rel.php.
[51] See, e.g., Symantec (2006). *Symantec Brightmail AntiSpam*. Retrieved November 5, 2006, from http://eval.veritas.com/mktginfo/enterprise/fact_sheets/ent-factsheet_brightmail_antispam_6.0_08-2004.en-us.pdf.
[52] Cole, William K. (2006, July 15). *Blacklists, Blocklists, DNSBL's, and Survival*. Retrieved October 23, 2006, from http://www.scconsult.com/bill/dnsblhelp.html.
[53] See, e.g., NJABL.org, *Remove an IP from the List.* Retrieved November 5, 2006, from http://njabl.org/remove.html.
[54] "Spammers are not people known for honesty, in fact they are almost all con men, fraudsters and chronic liars." Spamhaus. *ROKSO FAQ*. Retrieved October 23, 2006 from http://www.spamhaus.org/faq/answers.lasso?section=ROKSO%20FAQ#24.
[55] "Spamhaus regularly receives letters from spammers [sic] lawyers attempting to claim that all of a spammers [sic] records are in error and demanding all therefore be removed, [but] we naturally pay little attention to such requests." Id.
[56] See, e.g., CyberPromotions v. America Online, 948 F.Supp. 436 (1996); White Buffalo Ventures, LLC v. University of Texas, 420 F.3d 366 (5th Cir. 2005).
[57] Stratton Oakmont, Inc. v. Prodigy Services Co., 1995 WL 323710 (N.Y.Sup.,1995). (based upon Prodigy's automated filters, ability to edit posts and posting guidelines, court found Prodigy potentially liable for defamatory message board content).
[58] 47 U.S.C. § 230(b).

[59] 2000 WL 34016435 (Cal. Superior 2000).
[60] Cal. Bus. & Prof. Code § 17538.45 (2006).
[61] 2000 WL 34016435.
[62] "[S]tatements that are per se defamatory need not plead special damages; defamatory per se statements includes any statement that tends to damage a business reputation….."Spammer" and "spam" are disparaging labels in the Internet business community." Id.
[63] Media3 Technologies, LLC v. Mail Abuse Prevention System, LLC, 2001 WL 92389 (D.Mass. 2001) (Hosting company's request for preliminary injunction against MAPS in Massachusetts fails based on dispute over facts between parties).
[64] See, e.g., Cisneros, Oscar S. (2000, July 18). Yesmail Fights Blacklist Threat. *Wired News*. Retrieved October 22, 2006 from http://www.wired.com/news/politics/0,1283,37621,00.html.
[65] Gaspar, Suzanne (2001, October 26). E-mail marketer settles suit against MAPS. *Network World Fusion*. Retrieved November 5, 2006, from http://www.networkworld.com/news/2001/1026maps.html.
[66] Charny, Ben (2000, August 1). Harris Sues ISPs over Spam Blockade. *ZDNet News*. Retrieved November 5, 2006, from http://news.zdnet.com/2100-9595_22-522696.html.
[67] 323 F.Supp.2d 1037 (N.D.Cal. 2004).
[68] Subsequent to this case, Spamcop launched its own block list, making it more akin to MAPS and similar services. SpamCop. *SpamCop Blocking List*. Retrieved October 22, 2006, from http://spamcop.net/bl.shtml.
[69] 323 F.Supp.2d 1037 (N.D.Cal. 2004).
[70] Spamhaus. *ROKSO FAQ*. Retrieved October 23, 2006 from http://www.spamhaus.org/faq/answers.lasso?section=ROKSO%20FAQ#24.
[71] E360Insight (2006). *Case History*. Retrieved October 22, 2006 from http://www.e360insight.com/case_history.html.
[72] Spamhaus (2006). *Legal Answers & Updates*. Retrieved October 22, 2006, from http://www.spamhaus.org/legal/answer.lasso?ref=3.
[73] e360 Insight, LLC et al v. The Spamhaus Project, case # 1:06-cv-03958, available through the U.S. PACER electronic filings system at https://ecf.ilnd.uscourts.gov/.
[74] Answer of The Spamhaus Project, Ltd. To Complaint of e360, filed July 21, 2006.
[75] MOTION by Defendant Spamhaus Project, The to withdraw as attorney (Cripe, Andrew) (Entered: 08/21/2006).
[76] The Internet Corporation For Assigned Names and Numbers, which manages the allocation of .com, .org, .net and other top-level domain names. Retrieved October 22, 2006, from http://www.icann.org.
[77] U.S. District Court, Northern District of Illinois (2006, October 19). *Order*. Retrieved November 5, 2006, from http://www.icann.org/legal/spamhaus/denial-proposed_order-19oct06.pdf.
[78] 68 F.Supp.2d 692 (E.D.Va. 1999) (Virginia court found long-arm jurisdiction in defamation case over Maryland and New Mexico defendants, in part because defamation meant damage done in Virginia to Virginia-based plaintiff).
[79] 175 F.Supp.2d 367 (D. Conn 2001).

[80] Associated Press (2002, December 10). Aussie Can Sue Over Online Story. *Wired News*. Retrieved October 22, 2006, from http://www.wired.com/news/business/0,1367,56793,00.html.
[81] See "The Black Ice and OptInRealBig Cases: Exploring the Limits of 47 U.S.C. §230" supra.
[82] "Spammer" and "spam" are disparaging labels in the Internet business community." Mail Abuse Prevention System LLC v. Black Ice Software, 2000 WL 34016435, *7 (Cal. Superior 2000).
[83] E.g., Va. Code Ann. § 18.2-152.3:1 (described in note 15, supra).
[84] Rest 2d Torts § 558.
[85] Rest 2d Torts § 561.
[86] Rondeaux, Candace (2006, September 6). Anti-Spam Conviction Is Upheld. *Washington Post*, p. B03. (Jeremy Jaynes, convicted of sending tens of thousands of e-mails to AOL customers, sentenced to 9 years in prison).
[87] Rest 2d Torts §569, comments (d) and (e).
[88] Rest 2d Torts § 766B.
[89] Ferrill, A. Michael (1996). *Business Torts & Unfair Competition: A Practitioner's Handbook.* American Bar Association, 120-123 (summarizing California, Texas and Illinois versions of tort).
[90] "…SearsCarpet.com's e-mail server was blacklisted by MAPS without warning, stranding 25 telecommuters who couldn't send mail for two-and-a-half weeks and bouncing back 40% of outgoing e-mail messages. During a seven-week period, May's small IT department spent $25,000 in staff time trying to get off MAPS' blacklist and reconfigure 150 user workstations. All because a hacker used an open relay on May's network to send out millions of spam messages." Gaudin, Sharon and Gaspar, Suzanne (2001, September 10). The Spam Police. *NetworkWorld.* Retrieved November 4, 2006, from http://www.networkworld.com/research/2001/0910feat.html.
[91] "The Spamhaus Block List ("SBL") is a database of IP addresses from which Spamhaus does not recommend the acceptance of electronic mail - because they **appear to Spamhaus** to be under the control of, or made available for the use of, senders of Unsolicited Bulk Email ("spammers")." Spamhaus (2006). *SBL Advisory Rationale and Listing Criteria*. Retrieved October 22, 2006, from http://www.spamhaus.org/sbl/sbl-rationale.html (emphasis supplied).
See also Spews.org. *Frequently Asked Questions, Comments and Answers*. Retrieved October 22, 2006, from http://www.spews.org/faq.html.
[92] "Black Ice also alleges Mail Abuse blocked Black Ice's other servers, in addition to its mail server….This[sic] allegations, which are presumed true for demurrer purposes, do not plead a good-faith effort to block unsolicited bulk e-mail, but rather a bad-faith attempt to block solicited, individual e-mails." Mail Abuse Prevention System v. Black Ice, 2000 WL 34016435 (Cal. Superior 2000) at *9.
[93] McCaffery, Jen (2004, December 22). Missing Mail Found in Roanoke Residence. *The Roanoke Times*. Retrieved October 23, 2006, from http://www.roanoke.com/news/roanoke/wb/xp-15772).