Richmond Journal of Law and Technology

Volume 17 | Issue 2 Article 4

2011

Busting Blocks: Revisiting 47 U.S.C. § 230 to Address the Lack of Effective Legal Recourse for Wrongful Inclusion in Spam Filters

Jonathan I. Ezor

BUSTING BLOCKS: REVISITING 47 U.S.C. § 230 TO ADDRESS THE LACK OF EFFECTIVE LEGAL RECOURSE FOR WRONGFUL INCLUSION IN SPAM FILTERS

By Jonathan I. Ezor*

Cite as: Jonathan I. Ezor, *Busting Blocks: Revisiting 47 U.S.C. § 230 to Address the Lack of Effective Legal Recourse for Wrongful Inclusion in Spam Filters*, XVII RICH. J.L. & TECH. 7 (2011), http://jolt.richmond.edu/v17i2/article7.pdf.

I. INTRODUCTION: E-MAIL, BLOCK LISTS, AND THE LAW

[1] Consider a company that uses e-mail to conduct a majority of its business, including customer and vendor communication, marketing, and filing official documents. After conducting business in this manner for several years, one day the company discovers that its most recent e-mails were not delivered to recipients using a major Internet Service Provider ("ISP") because the company was recently listed on an automated block list as a sender of unwanted bulk commercial e-mail ("spam").[1] The

* Assistant Professor of Law and Director, Institute for Business, Law and Technology, Touro College Jacob D. Fuchsberg Law Center, Central Islip, NY. The author wishes to acknowledge the invaluable help of Jerry Simon and Andrew Van Singel in the preparation of this article. Earlier drafts of this article were posted at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=944551, presented at the International Association of IT Lawyers' December 2006 International Conference at Business, Law and Technology, *available at* http://www.iblt.eu/IBLT2006/ (last visited July 23, 2010), and published in the proceedings for that conference.

[1] *See Jargon Buster*, OFF. FOR INTERNET SAFETY, http://www.internetsafety.ie/website/ois/oisweb.nsf/page/48AF34B2EDEF4B77802574C70054D7D1 (last visited Jan. 18, 2011).

company's status on the block list affects not only marketing e-mails, but all e-mails sent from the business's server.[2] Worse still, an overseas organization, rather than the company's ISP, controls the block list, and its policy is to disregard complaints of improper blocking from anyone other than an e-mail sender's ISP.[3]

[2] Now imagine a marketer that utilizes third-party affiliates to reach a broader customer base.[4] The marketer provides its affiliates with guidelines regarding proper marketing techniques, including refraining from sending spam, but, despite the marketer's efforts, one affiliate distributes unsolicited e-mail messages. It is reasonable to suggest that the affiliate employing the unauthorized marketing technique will end up on a block list, but what about the marketer?

[3] Next, consider an ISP's customers. While the majority of those customers practice responsible modes of e-marketing, one chooses to send out millions of spam messages. Rather than identifying and sanctioning the rouge spammer, the block list operator places all of the ISP's customers on the block list.[5]

---

[2] *See What are Blacklists?*, MAILCHIMP, http://www.mailchimp.com/kb/article/what-are-blacklists/ (last updated Dec. 2, 2009).

[3] Given the nature of the service, block list operators likely will not address complaints from a blocked sender without some reassurance (i.e. confirmation from an ISP) that the sender is not a spammer. *See Frequently Asked Questions (FAQ), ROKSO FAQ,* SPAMHAUS, http://www.spamhaus.org/faq/answers.lasso?section=ROKSO%20FAQ#24 (last visited Jan. 16, 2011) [hereinafter *ROKSO FAQ*] ("Spamhaus regularly receives letters from spammer's [sic] lawyers attempting to claim that all of a spammers [sic] records are in error and demanding all therefore be removed. [Spamhaus] naturally pay[s] little attention to such requests.").

[4] *See Affiliate Marketing*, ENTREPRENEUR, http://www.entrepreneur.com/encyclopedia/term/82092.html, (last visited Jan. 27, 2011) (defining Affiliate Marketing as "[a] way for a company to sell its products by signing up individuals or companies ('affiliates') who market the company's products for a commission. There are two ways to approach affiliate marketing: You can offer an affiliate program to others or you can sign up to be another business's affiliate.").

[5] *See* Carl Brooks, *Cloud Computing News: Amazon EC2 Email Blocked by Antispam Group Spamhaus*, SEARCHCLOUDCOMPUTING.COM (Oct. 14, 2009),

[4] Finally, picture an ISP that assigns a new customer an Internet Protocol ("IP") address formerly issued to a spammer.[6] When the new customer tries to send an e-mail, she discovers that she is unable to do so because the previous user's spamming activities condemned the IP address to a block listing.[7]

[5] In the preceding hypotheticals, those improperly placed on a block list may well pursue the following course of action to remedy the situation. First, the parties may seek to work with their ISPs to resolve the problem.[8] If the ISP is unable or unwilling to assist in the matter, the parties will likely request the block list operator to remove them from the block list.[9] If this endeavor proves unsuccessful, possibly because the block list operator is unwilling to communicate with "spammers," is

---

http://searchcloudcomputing.techtarget.com/news/1371369/Amazon-EC2-email-blocked-by-antispam-group-Spamhaus.

[6] Every device connected to the Internet is given a unique numerical address, the Internet Protocol ("IP") address, to allow identification by, and communication with, other connected devices. *See* GERHARD RUFA, DEVELOPMENTS IN TELECOMMUNICATIONS, 60 (2008). ISPs, for example, are granted blocks of IP addresses by one of five Regional Internet Registries ("RIR"), including the American Registry for Internet Numbers ("ARIN"), which receives the authority to allocate IP addresses from the Internet Assigned Numbers Authority ("IANA"), a single recognized global body. *See Number Resource Policy Manual*, AM. REGISTRY FOR INTERNET NUMBERS, 3 (Sept. 9, 2010), https://www.arin.net/policy/nrpm.pdf. An ISP, having been issued a finite list of IP addresses to provide to its customers, may choose either static (one IP address per subscriber) or dynamic (IP addresses no longer in use are re-allocable for future use) IP address allocation. *Cf. Internet Registry IP Allocation Guidelines, RFC 2050*, INTERNET ASSIGNED NUMBERS AUTHORITY, 6 (Nov. 1996), http://www.rfc-editor.org/rfc/pdfrfc/rfc2050.txt.pdf.

[7] *See infra* notes 152-65 and accompanying text (discussing the difficulty associated with obtaining removal from a block list).

[8] *See* Zeran v. Am. Online, Inc., 129 F.3d 327, 329 (4th Cir. 1997).

[9] *See* Pallorium, Inc. v. Jared, No. G036124, 2007 WL 80955, *2 (Cal. Ct. App. Jan., 11 2007).

unreachable via any reasonable means, or simply chooses not to remove the victim from the list, the parties likely will turn to the courts.[10]

[6] Claims resulting from improper spam blocking typically fall under the category of traditional business tort litigation, particularly if the affected organization is unable to operate its business, loses opportunities, or misses mandatory legal deadlines because of its restricted access to its e-mail services.[11] However, following the passage and interpretation of 47 U.S.C. § 230, *et seq.*, which is codified under the Communications Decency Act ("CDA")[12] and seeks to encourage Internet growth while

[10] *See id.*

[11] *See* RESTATEMENT (SECOND) OF TORTS §§ 766-74 (1979) (outlining the long history of business tort litigation in which companies that suffer loss are eligible to receive monetary or equitable remedies to undo or at least mitigate the damage); *infra* Part VIII (discussing potential commercial claims for wrongful block listing).

[12] The Communications Decency Act of 1934 ("CDA") was enacted as part of the Telecommunications Act of 1996, *see* Telecommunications Act of 1996, Pub. L. No. 104-104, 110 Stat. 56, in response to cases such as *Stratton Oakmont, Inc. v. Prodigy Services Co.,* No. 31063/94, 1995 N.Y. Misc. LEXIS 229 (N.Y. Sup. Ct. May 24, 1995), which drew significant criticism for arguably holding all online content providers liable under defamation law for everything third parties place on their sites or services, requiring providers to fact-check each posting or remove the ability of third parties to add content. *See* Zango, Inc. v. Kaspersky Lab, Inc., 568 F.3d 1169, 1173 (9th Cir. 2009) (citing a statement in the House Conference Report that overruling *Stratton Oakmont* was "one of the specific purposes" of 47 U.S.C. § 230) (citation omitted) (internal quotation marks omitted); Susan Benkelman, *Watch Your Talk, Online Cops Walk Thin Line in Monitoring*, NEWSDAY, Dec. 26, 1995, at A8 (discussing the challenges before online services with respect to monitoring in light of the seemingly conflicting concepts of Congress and the *Prodigy* case). CDA's main provisions amended 47 U.S.C. § 223 to prohibit the transmission of "obscene or indecent" material to recipients under 18, and were challenged by the American Civil Liberties Union and ultimately held unconstitutional. *See generally* Reno v. ACLU, 521 U.S. 844 (1997). But, § 509, the portion of the CDA at issue in this article, was not challenged in *Reno* and remains valid and enforceable. *See* 47 U.S.C. § 203 (2006). *See generally* Reno v. ACLU, 521 U.S. 844 (1997).

focusing protection on user-created and distributed material,[13] business tort litigation does not provide an easy cure to improper block listings.[14]

[7] Title 47, section 230(c) of the United States Code provides that:

> (1) . . . 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) . . . 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).[15]

Subsection (e)(3) goes on to state in relevant part that, "[n]o cause of action may be brought and no liability may be imposed under any State or local law that is inconsistent with this section."[16]

[8] While the initial context of 47 U.S.C. § 230 targeted defamation via message boards, some courts have interpreted the statute broadly to

---

[13] *See* 47 U.S.C. § 230(b) (2006).

[14] *See Pallorium*, 2007 WL 80955, at *5.

[15] 47 U.S.C. § 230(c) (2006). Note that the reference to "paragraph (1)" appears erroneous and meant instead to refer to subsection (c)(2)(A). *Id.* §230(c)(2) n.1; *Zango*, 568 F.3d at 1173 n.5 ("We take it that the reference to the 'material described in paragraph (1)' is a typographical error, and that instead the reference should be to paragraph (A), i.e., § 230(c)(2)(A).") (emphasis omitted).

[16] 47 U.S.C. § 230(e)(3) (2006).

cover a range of situations where one party places content on another party's server or web site.[17] The statute essentially immunizes an ISP taking steps to protect its users from objectionable content, and finds its rationale in the belief that granting such immunity will encourage productive, safe Internet resources.[18] Common among statutes designed to address the Internet and other advanced technologies, the drafters' intent and statutory language may not have adequately anticipated future technological and business developments.[19] Thus, the language and jurisprudence of 47 U.S.C. § 230, its second section in particular, produce the result that block list providers are largely untouchable in court.[20]

[9] The precedent surrounding 47 U.S.C. § 230 makes it unlikely that courts will significantly diverge from the current understanding and

---

[17] *See, e.g.*, Zeran v. Am. Online, Inc., 129 F.3d 327, 330 (4th Cir. 1997) (applying 47 U.S.C. § 230 where the plaintiff filed against an online service provider after a third party posted false, offensive advertisements that included the plaintiff's contact information). The court noted that "[b]y its plain language, § 230 creates a federal immunity to any cause of action that would make service providers liable for information originating with a third-party user of the service." *Id.*

[18] *See* 47 U.S.C. § 230(c); *Zeran*, 129 F.3d at 330-31; David S. Ardia, *Free Speech Savior or Shield for Scoundrels: An Empirical Study of Intermediary Immunity Under Section 230 of the Communications Decency Act*, 43 LOY. L.A. L. REV. 373, 410-11 (2010).

[19] *See e.g.*, 18 U.S.C. § 1084 (2006). In *In re MasterCard Int'l Inc.*, the Fifth Circuit affirmed the district court's judgment that defendant credit card companies' involvement with internet gambling websites did not violate the Racketeer Influenced and Corrupt Organizations Act ("RICO") or the Wire Act. 313 F.3d 257, 263 (5th Cir. 2002). The court reasoned that because the Wire Act did not outlaw internet gambling websites, the RICO Act did not apply and summary judgment was granted to the credit card companies. *Id.*

[20] *See, e.g.*, Pallorium, Inc. v. Jared, No. G036124, 2007 WL 80955, *1 (Cal. Ct. App. Jan. 11, 2007) (finding a block list provider immune under 47 U.S.C. § 230(c)(2)). The policy discussion of Ardia's study (like most of the cases addresses in his article) focuses on subsection (c)(1) of 47 U.S.C. § 230, a service provider's immunity against liability for another party's content. *See* Ardia, *supra* note 18, at 412 n.194. As this Article demonstrates, it is subsection (c)(2) that more directly addresses the activities of major block list providers, as the brevity and lack of substantive due process requirements lead to a lack of recourse for those improperly placed on block lists. *See* 47 U.S.C. § 230(c)(2).

breadth of immunity the statute grants block list providers.[21] An appropriate remedy to this issue requires statutory revision that will establish a more reasonable and objective standard to delineate the conduct of block list operators and communicative third-party vendors, and set forth procedural avenues through which an aggrieved party may seek to rectify an incorrect block listing or obtain assistance from the courts. The Digital Millennium Copyright Act ("DMCA") provides a model for such revision, as it grants site owners an analogous safe harbor for copyright liability from third-party content,[22] and, unlike 47 U.S.C. § 230, mandates that site owners comply with all necessary prerequisites and implement adequate procedures to obtain protection.[23] Admittedly inexact for comparison, some DMCA procedures may be burdensome given the volume of parties the major block lists impact.[24] However, such practices remain preferable to the subjective policies and arbitrary decisions currently in place among block list operators, who manage access to millions of personal and professional inboxes throughout the world.[25]

[10] Spam is a true Internet plague. It slows down systems, clogs storage devices, and makes it difficult for users to find desired messages in a sea of solicitations for questionable medical products, ways to "make money fast," offers for companionship, and other unsolicited pitches.[26] Efforts to grant service providers and users some level of control over the volume and type of messages they receive, by both technologists and legislators, have done much toward maintaining e-mail as a useful

---

[21] *See infra* Part VIII.

[22] 17 U.S.C. § 512(b)-(c) (2006).

[23] *Id.* § 512(i).

[24] *See, e.g.*, *About Spamhaus*, SPAMHAUS, http://www.spamhaus.org/organization/index.lasso (last visited Jan. 27, 2011) ("The number of internet users whose mailboxes are currently protected by Spamhaus DNSBLs now exceeds 1.4 Billion.").

[25] *See id.*

[26] *See Spam Scams*, SPAMLINKS, http://spamlinks.net/scams.htm (last visited Jan. 17, 2011) (listing and describing common spam scams)

resource.[27] Nevertheless, the current state of the law denies those who have been block listed – spammers and non-spammers alike – adequate due process with respect to their dealings with block list operators, or a guaranteed right to judicial redress.[28]

II. A SHORT HISTORY OF SPAM

[11] To better understand the problems associated with 47 U.S.C. § 230, it is instructive to review the history and current status of spam, and the efforts of those who seek to minimize it. Originally, the Internet and e-mail were intended as educational, government tools.[29] In fact, the Acceptable Use Policy of the National Science Foundation restricted commercial use of the Internet well into the 1990's.[30] Following the removal of the Acceptable Use Policy restriction, commercial exploitation of the Internet, including electronic mail and the spread of unsolicited bulk commercial messages, which quickly earned the nickname spam,[31] erupted.[32]

---

[27] *See* Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003, Pub. L. No. 108-187, 117 Stat. 2699 ("CAN-SPAM"); SPAMHELP, http://www.spamhelp.org (last visited Jan. 17, 2010) (providing information on available software and legislation that allow users to avoid spam).

[28] *See* discussion *infra* Part IX.A. Often, victims of improperly block listings wind up on block lists because of an accidental inclusion or as a means of exercising leverage over an ISP to stop facilitating spamming. *See* Brooks, *supra* note 5.

[29] *See* Timothy Coughlan, *Applying the U.S. Postal Service Statutes to E-Mail Transmissions*, 25 RUTGERS COMPUTER & TECH. L.J. 375, 379-83 (1999); Keith J. Epstein & Bill Tancer, *Enforcement of Use Limitations by Internet Service Providers: "How To Stop That Hacker, Cracker, Spammer, Spoofer, Flamer, Bomber"*, 19 HASTINGS COMM. & ENT. L.J. 661, 663 (1997).

[30] *See* Epstein & Tancer, *supra* note 29; *see also A Timeline of NSF History*, NAT'L SCI. FOUND., http://www.nsf.gov/about/history/timeline90s.jsp#1990s (last visited Jan. 17, 2011).

[31] *See* DAVID CRYSTAL, LANGUAGE AND THE INTERNET 53 (2001) ("The origin of the term ["spam"] lies in a 1970 *Monty Python* sketch in which a cafe waitress describes the available dishes to two customers, and culinary variation is introduced by an increasing reliance on spam . . . ."); *see also* Roger Allan Ford, *Preemption of State Spam Laws by*

[12] Although the first spam e-mail reportedly occurred as early as 1978,[33] the first widely recognized spam occurrence transpired on March 5, 1994 on Usenet, the topical message boards mirrored across the Internet.[34] It was not until the late 1990's that e-mail spam, a scourge of users and network administrators alike, began to build serious momentum.[35] As the frequency and amount of spam increased, consumers pressured service providers, software vendors and the legal system to reduce the burden, particularly because of the costs consumers incurred.[36]

[13] Prior to the development of spam e-mail, there had been little need to develop anti-spam legislation because the marketers of offline, bulk commercial mail bore the costs associated with standard mail delivery.[37] The development of spam e-mail provided marketers with the opportunity to shift the costs to the consumer, thereby allowing the marketers to send

---

the Federal CAN-SPAM Act, 72 U. CHI. L. REV. 355, 355 (2005) ("More than thirteen billion spam messages are sent per day.").

[32] JONATHAN EZOR, CLICKING THROUGH: A SURVIVAL GUIDE FOR BRINGING YOUR COMPANY ONLINE 138-39 (2000) (explaining the explosive growth of unsolicited commercial e-mail by way of a hypothetical that illustrates the high rate of return on investment that cannot exist with traditional mail services); *see also* Richard M. Smith, *The Web Bug FAQ*, ELECTRONIC FRONTIER FOUND. (Nov. 11, 1999), http://w2.eff.org/Privacy/Marketing/web_bug.html (explaining mass e-mail marketers' use of "web bugs," invisible graphics that collect real time information about the effectiveness of an advertisement, including deletion of addresses that do not view the content).

[33] Tony Long, *May 1, 1978: Spam, From Novelty to Nuisance in a Couple of Decades*, WIRED, (May 1, 2007) http://www.wired.com/science/discoveries/news/2007/05/dayintech_0501; *see also* Brad Templeton, *Reaction to the DEC Spam of 1978*, TEMPLETONS, http://www.templetons.com/brad/spamreact.html (last visited Jan. 17, 2011).

[34] Glyn Moody, *Spam's Tenth Birthday Today*, NETCRAFT (Mar. 5, 2004), http://news.netcraft.com/archives/2004/03/05/spams_tenth_birthday_today.html.

[35] *Cf.* Amy G. Marino, *Is Spam the Rock of Sisyphus?: Whether the Can-Spam Act and Its Global Counterparts Will Delete Your E-Mail*, 32 PEPP. L. REV. 1021, 1025 (2005).

[36] *See id.* (noting that most Internet users paid by the minute).

[37] *See id.* at 1024-25.

more solicitations with less overhead.[38] Eventually, the burdens stemming from the rising levels of commercial bulk e-mail drove Internet users to seek legal remedy.[39]

[14] The legal system had difficulty curbing the growth of spam, as there were few cases on point, and the little precedent that did exist, was relatively unclear.[40] Initially, spam recipients and ISPs seeking legal redress were limited to adapting existing offline doctrines to address the unauthorized use of servers and computers as bulk e-mail conduits.[41] But, the need to adapt the existing law quickly became apparent.[42]

[15] In early cases, plaintiffs crafted their cause of action through analogy to existing doctrine, for example, trespass to chattel, because the law had not yet established a cause of action for claims stemming from commercial bulk e-mailings.[43] While some trespass to chattel claims, particularly those brought by ISPs, were successful,[44] other cases, such as *Intel v. Hamidi*,[45] found United States courts less than willing to extend the doctrine to e-mail. The difficulty and uncertainty associated with

---

[38] *Id.* at 1025.

[39] *See id.* at 1025-29.

[40] *See generally id.* (discussing the development of Federal and State anti-spam legislation, and constitutional and procedural concerns associated with claims against spammers).

[41] *See id.* at 1025-26, 1029.

[42] *See id.* at 1024-26.

[43] *See, e.g.*, CompuServe Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015, 1020 (S.D. Ohio 1997) (claiming trespass to chattels); *see also* Hotmail Corp. v. Van$ Money Pie Inc., C-98 JW PVT ENE, C 98-20064 JW, 1998 WL 388389, *6-7 (N.D. Cal. Apr. 16, 1998) (claiming trespass to chattel, breach of contract and fraud and misrepresentation).

[44] *See, e.g.*, *Compuserve*, 962 F. Supp. at 1023.

[45] 71 P.3d 296, 308 (Cal. 2003) (holding that a former employee who sent thousands of critical e-mail messages to his ex-employer's e-mail system was not liable for trespass to chattels).

arguing these claims, made it clear that a more specific legislative approach might be needed.[46]

III. THE RISE OF SPECIFIC ANTI-SPAM LEGISLATION

[16] Eventually, legislatures took up the effort against spam, both in individual states,[47] and at the federal level via the CAN-SPAM Act.[48] Before Congress enacted CAN-SPAM, critics expressed doubt that lawmakers would be able to reduce the deluge of spam infiltrating users inboxes.[49] The criticism arose for two reasons. First, the Internet is

---

[46] Similarly, the issue of addressing cybersquatting through traditional trademark law led to the passage of the Anticybersquatting Consumer Protection Act in 1999 ("ACPA"). *See* Anticybersquatting Consumer Protection Act, Pub. L. No. 106-113, 113 Stat. 1501, app. I 1501A-521 (1999), *codified at* 15 U.S.C. § 1125. Trademark holders who believed their rights were violated sued under theories of unfair competition, infringement, and dilution, attempting to hold domain name registrars liable for issuing infringing domain names. *See, e.g.*, Lockheed Martin Corp. v. Network Solutions, Inc., 194 F.3d 980, 986-87 (9th Cir. 1999) (finding a domain name registrar not liable for registering a domain that allegedly infringed the plaintiff's trademarks); Avery Dennison Corp. v. Sumpton, 189 F.3d 868, 880-81 (9th Cir. 1999) (finding against an office supplies company in its trademark dilution claim against a registrant of domains based upon last names that included "Avery" and "Dennison"); Brookfield Commc'ns, Inc. v. W. Coast Entm't Corp., 174 F.3d 1036, 1066 (9th Cir. 1999) (finding in favor of an entertainment services provider that brought a trademark infringement case against a video rental chain for using "MovieBuff" as a domain name). In response to the growing number of cases on these issues and the lack of specific statutory guidance, Congress enacted the ACPA. *See* Pub. L. No. 106-113, 113 Stat. 1501, app. I 1501A-521 (1999), *codified at* 15 U.S.C. § 1125; Coca-Cola Co. v. Purdy, 382 F.3d 774, 778 (8th Cir. 2004). ACPA added a new section to the Lanham Act, the United States federal trademark law, which established a private cause of action and statutory damages "bad faith" cybersquatting. *See* 15 U.S.C. § 1125(d) (2006).

[47] *See Summary*, SPAM LAWS, http://www.spamlaws.com/state/summary.shtml (last visited Jan. 17, 2011) (providing a state-by-state summary of spam laws).

[48] Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003, Pub. L. No. 108-187, 117 Stat. 2699 ("CAN-SPAM").

[49] *See* Declan McCullagh, *FTC Chair: Antispam Proposals Lacking*, CNET NEWS (Aug. 19, 2003), http://news.com.com/FTC+chair+Antispam+proposals+lacking/2100-1028_3-5065739.html.

international and thus purely local, and even national, law would have little affect against offshore spammers.[50] Second, spam is largely the province of small, unsophisticated, or "guerrilla" marketers, rather than large corporations with both assets at risk and legal departments to advise them regarding compliance with the law.[51] Critics also noted the practical challenge of identifying what "spam" truly is; one user's unsolicited commercial bulk e-mail message may be another's "just what I wanted" offer.[52]

[17] Anti-spam statutes have in large part sidestepped the definitional issues and instead focus on labeling advertisements, prohibiting misleading techniques (such as disguising the sender's identity or disregarding unsubscribe requests by unwilling recipients), and requiring proper sender identification.[53] Even with this approach, defining what constitutes advertising poses its own problems, since an e-mail message may include both advertisement and informational material.[54] How, for example, should the law characterize a newsletter that 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" in most recipients' views.[55]

---

[50] *See* David Chartier, *First Spam Felony Conviction Upheld: No Free Speech to Spam*, ARS TECHNICA (Mar. 2, 2008), http://arstechnica.com/tech-policy/news/2008/03/first-spam-felony-conviction-upheld-no-free-speech-to-spam.ars (alluding to CAN-SPAM's limited reach).

[51] *See* Paul Roberts, *EarthLink Wins $16 Million in Spam Case*, PCWORLD (May 7, 2003), http://pcworld.com/article/id,110627-page,1/article.html.

[52] *See* Cindy Cohn & Annalee Newitz, *Noncommercial Email Lists: Collateral Damage in the Fight Against Spam*, ELECTRONIC FRONTIER FOUND. (Nov. 2004), http://www.eff.org/wp/noncommercial-email-lists-collateral-damage-fight-against-spam.

[53] *See, e.g.*, 15 U.S.C. § 7704 (2006) (enacting part of CAN-SPAM).

[54] *See* Erika Hallace Kikuchi, *Spam in A Box: Amending Can-Spam & Aiming Toward A Global Solution,* 10 B.U. J. SCI. & TECH. L. 263, 268 (2004).

[55] *See* Grant Yang, *Can-Spam: A First Step to No-Spam*, 4 CHI.-KENT J. INTELL. PROP. 1 (2004).

[18] Enforcement is another major hurdle confronting anti-spam legislation.[56] A proposed statute intended to regulate spam must address issues of jurisdiction (interstate and international), both to bring the alleged spammer before the court, and to enforce any assessed penalties.[57] Before establishing jurisdiction, though, the enforcement agency or litigant must identify the spammer.[58] This is not a simple process, as the Internet enables both anonymity[59] and pseudonymity,[60] factors that can be further complicated by the spamming tactic of falsifying an e-mail's identifying information.[61] While some enforcement methods may work, it is still relatively simple for even an in-jurisdiction spammer to hide his tracks.[62] Also, spammers frequently change ISPs and accounts as tracking efforts get closer to them.[63] Furthermore, even if found, a spammer may

---

[56] Meyer Potashman, *International Spam Regulation & Enforcement: Recommendations Following the World Summit on the Information Society*, 29 B.C. INT'L & COMP. L. REV. 323, 332-37 (2006); *see also* Yang, *supra* note 52.

[57] Elizabeth A. Alongi, Note, *Has the U.S. Canned Spam?*, 46 ARIZ. L. REV. 263, 281-84 (2004); *see also* Kenneth C. Amaditz, *Canning "Spam" in Virginia: Model Legislation to Control Junk E-Mail*, 4 VA. J.L. & TECH. 4, 52-60 (1999).

[58] *See* Amaditz, *supra* note 57, at 60.

[59] *See, e.g.*, *Anonymous Web Surfing with Anonymizer Universal*, ANONYMIZER, http://www.anonymizer.com/universal (last visited Jan. 17, 2011) (discussing a product that enables anonymous Internet browsing); *see also Anonymity Online*, TOR, http://torproject.org/ (last visited Jan. 12, 2011) (discussing an anonymous Internet communications system).

[60] Andreas Pfitzmann & Marit Hansen, Anonymity, Unlinkability, Unobservability, Pseudonymity, and Identity Management – A Consolidated Proposal for Terminology, 13-14 (2005), *available at* http://www.freehaven.net/anonbib/cache/terminology.pdf (defining pseudonymity as "the use of pseudonyms as IDs").

[61] *See* Roberts, *supra* note 51.

[62] *See* Charles Arthur, *Will Convicting Five Major Spammers Put an End to Spam?*, GUARDIAN (June 24, 2009), http://www.guardian.co.uk/technology/2009/jun/24/spam-newly-asked-questions (discussing United States based spammers using foreign servers to distribute their spam).

[63] *See* Roberts, *supra* note 51 (describing how EarthLink pursued spammer Howard Carmack and "shut down several accounts he used").

well be judgment proof or have otherwise hidden his assets.[64] Finally, even in jurisdictions where spamming is a felony, as in Virginia,[65] convictions are rare.[66]

IV. BLOCK LISTS AND SPAM FILTERS: SELF-REGULATION THROUGH TECHNOLOGY

[19] Before legislators took up the fight against spam, Internet users employed two main methods to address the problem: block listing and filtering.[67] Block listing began as a way to educate the public and name (thereby effectively shaming) the most egregious spammers.[68] Paul Vixie's "Real-time Blackhole List" was one of the first block list resources.[69]

---

[64] *See* Associated Press, *AOL Wants to Dig for Gold in Spammer's Parents' Back Yard*, FOXNEWS.COM (Aug. 17, 2006), http://www.foxnews.com/story/0,2933,208712,00.html (explaining AOL's plans to dig in the backyard of the parents of a convicted spammer who was facing a $12.8 million judgment in hopes of finding gold and platinum bars he might have buried there).

[65] VA. CODE ANN. § 18.2-152.3:1 (Supp. 2010) (identifying spamming as a misdemeanor, or, if transmission or revenue exceeds certain levels, a class 6 felony).

[66] *See, e.g.*, Chartier, *supra* note 50 (discussing the Virginia Supreme Court's decision to uphold the 2008 conviction of Jeremy Jaynes, the *first* felony spamming conviction in the United States). At least one major convicted spammer has been imprisoned. Hibah Yousuf, *'Godfather of Spam' Going to Prison*, CNNMONEY.COM (Nov. 24, 2009), http://money.cnn.com/2009/11/24/technology/King_of_spam_lawsuit_fraud_Ralsky/index.htm (discussing the November 2009 conviction of Alan Ralsky under the federal CAN-SPAM Act, and his subsequent fifty-one month sentence).

[67] *See* Neil Schwartzman, *Trench Warfare in the Age of the Laser-Guided Missile*, (Jan. 16, 2007, 7:25 AM), http://www.circleid.com/posts/anti_spam_virus_trench_warfare/.

[68] *See What is a DNSBL?*, DNSBL.INFO, http://www.dnsbl.info/, (last visited Jan. 27, 2011) ("DNS Blacklists have a rather long history in web terms, with the first one being created in 1997. Called the RBL, its purpose was to block spam email and to educate Internet service providers and other websites about spam and its related problems.")

[69] *See* Robert McMillan, *What Will Stop Spam? Paul Vixie Hopes His Realtime Blackhole List Will at Least Be a Start*, SUNWORLD (Dec. 1997), http://sunsite.uakom.sk/sunworldonline/swol-12-1997/swol-12-vixie.html (interviewing Paul Vixie regarding the development of his Realtime Blackhole List).

[20] At the outset, Vixie's block list was a reference users employed to identify and block senders on a sender-by-sender basis.[70] As Internet and e-mail usage expanded to include the everyday consumer, and spam became a more widespread problem, the Internet community began to scale up its blocking efforts.[71] The block list evolved into a downloadable, standardized tool that ISPs could connect to their servers, thereby importing the entire block list (which was regularly updated), and block all e-mail from senders the list designated as spammers.[72]

[21] Several block lists are volunteer-maintained, such as The Spamhaus Project ("Spamhaus"), which is based in the United Kingdom.[73] Others, like Julian Haight's SpamCop, were originally volunteer efforts, but were eventually sold to commercial e-mail security firms.[74] Vendors, such as Symantec, offer software that incorporates block lists, running either on an ISP's private mail server or remotely via a shared application service provider ("ASP") model.[75]

[22] Block lists populate their spammer databases in a number of ways. One method is that list managers set up accounts or networks on popular ISPs that "probe" for spam but are otherwise unused.[76] Spammers using a technique called "dictionary attacks," in which spammers send bulk

---

[70] *See id.*

[71] *See id.*

[72] *See id.*

[73] *See About Spamhaus*, SPAMHAUS, http://www.spamhaus.org/ (last visited Jan. 17, 2010).

[74] *See SpamCop FAQ: What is SpamCop's History?*, SPAMCOP.NET, http://www.spamcop.net/fom-serve/cache/109.html (last visited Jan. 17, 2011).

[75] *Symantec Brightmail AntiSpam, Advanced Antispam and Email Security Solution for the Enterprise,* SYMANTEC, http://eval.veritas.com/mktginfo/enterprise/fact_sheets/ent-factsheet_brightmail_antispam_6.0_08-2004.en-us.pdf (last visited Oct. 28, 2010).

[76] Nathan Segal, *Filtering Spam with Blocklists*, SMALL BUS. COMPUTING.COM, (Sept. 22, 2002), http://www.smallbusinesscomputing.com/webmaster/article.php/1467881.

commercial messages to every conceivable combination of numbers and letters for possible e-mail addresses, unknowingly include the trolling accounts.[77] Once the account receives a commercial message, the message's details are added to the overall block list.[78]

[23] Another method focuses on the servers that send the e-mail. Outgoing e-mail servers may either reject messages coming from outside their network or subscriber population, or pass the outside messages along to their destinations.[79] Those that indiscriminately pass along messages are "open relays," and spammers frequently utilize them to disguise the origin of unsolicited advertising.[80] Given this risk, anti-spam proponents have sought to encourage the elimination of open relays through the creation of public open relay block lists,[81] as well as other block lists of similar outside-access exploits.[82] Even when a server is not open to the public, if its authorized users utilize it to send spam, the server, and all of its customers, spammers and non-spammers alike, may be added to block lists, causing problems for everyone.[83] This possibility is of particular importance to ISPs that offer connectivity services to company networks as well as individual users.[84] ISPs that use technical means to disable

[77] *See Dictionary Attack Spam*, ONLYMYEMAIL ANTI-SPAM BLOG, http://blog.onlymyemail.com/dictionary-attack-spam/ (last visited Jan. 17, 2011).

[78] *See* Segal, *supra* note 76.

[79] *See* Joseph Neubauer, *Fortify Your Email Transport – Part 2*, MICROSOFT (June 21, 2002), http://technet.microsoft.com/en-us/library/cc750375.aspx.

[80] *See id.*

[81] *See* Matthew Broersma, *Spam Project Pulls Plug, Open-Relay Volunteer Monitors Hang It Up*, COMPUTERWORLD (Dec. 21, 2006), http://www.computerworld.com/s/article/9006578/Spam_project_pulls_plug (discussing a former anti-spam blacklist service, the Open Relay Database ("ORDB"), which distributed a blacklist of mail servers that allowed open relays and were therefore prone to spamming).

[82] *See, e.g.*, *XBL Advisory, Exploits Block List*, SPAMHAUS, http://www.spamhaus.org/XBL/ (last visited Jan. 12, 2011).

[83] *See* Cohn & Newitz, *supra* note 52.

[84] *See id.*

connecting mail servers in order to prevent the ISP from being deemed "spammer friendly," can inconvenience legitimate high-volume mailers and corporate customers.[85]

[24] A third method used to populate block lists is collaborative reporting.[86] Through this method, users report spam to block lists, either through an e-mail message to the operators,[87] or via an on-screen button in an e-mail program.[88] Depending on how the block list functions, the information may be immediately added to the block list or investigated further.[89] The advantage of collaboration is that it extends the net through which spam is caught far beyond the reach of list manager. With some additional tools, the community collaborating on reporting ideally gets the benefit of stronger and more accurate spam blocking.[90]

[25] In parallel with the rise of shared block lists, e-mail programs also offer internal spam filters.[91] Microsoft's Outlook e-mail program, for example, began offering a "junk mail" filter with its Outlook 98 version,

---

[85] *See id.*

[86] *See SpamCop FAQ: How Does SpamCop Reporting Work?*, SPAMCOP.NET, http://www.spamcop.net/fom-serve/cache/3.html (last visited Jan. 17, 2011).

[87] *See id.* (describing how the SpamCop service utilizes user reporting to identify spam, then communicates with the spammer's service provider).

[88] *See How It Works*, CLOUDMARK DESKTOPONE, http://www.cloudmarkdesktop.com/en/home (last visited Jan. 17, 2011) (discussing Cloudmark DesktopOne, a spam-blocker that surveys user feedback in Microsoft Outlook and Outlook Express and uses the feedback to generate block lists).

[89] *See SpamCop FAQ: How Does SpamCop Reporting Work?*, *supra* note 86.

[90] According to the Cloudmark software program on the author's computer, for example, as of October 3, 2006, the Cloudmark Desktop collaborative filter had checked 3,585,957,863 messages, with 75,214,674 spam messages "blocked by the community" and 1,729,376,093 "automatically stopped."

[91] *See OL98: How to Filter Junk and Adult Content E-mail*, MICROSOFT (Mar. 6, 2001), http://support.microsoft.com/?kbid=182251.

which based its filtering on a combination of suspect terms and user feedback (i.e. labeling a message as "junk mail," which thereafter routed the sender's messages to a Junk Mail or Deleted Items folder).[92]

[26] As spammers' e-mail modification techniques become more sophisticated (including falsifying sender information), and adapt to beat the simpler blocking methods, software-based filters must incorporate more heuristic methodologies, such as analyzing words, punctuation, sender information, mail server information, and other elements to score incoming messages as spam.[93] This method, called Bayesian filtering,[94] is based on work of the eighteenth century theoretician Rev. Thomas Bayes.[95] Once the software scores the incoming message, the user or ISP may choose whether to label a message as suspected spam, redirect it to a dedicated spam folder, or automatically delete it.[96]

V. SPAM(MER) LABELING AND THE CHALLENGE OF FALSE POSITIVES

[27] The processes that filter messages and identify spam are not perfect. The first challenge is definitional.[97] Just as United States

---

[92] *See id.*

[93] *See* Paul Hoffman & Dave Crocker, UNSOLICITED BULK E-MAIL: MECHANISMS FOR CONTROL, INTERNET MAIL CONSORTIUM, (May 4, 1998), http://www.imc.org/ube-sol.html; Paul Graham, *A Plan for Spam*, PAUL GRAHAM (Aug. 2002), http://www.paulgraham. com/spam.html.

[94] *See* Hoffman & Crocker*, supra* note 93; Graham, *supra* note 93.

[95] *See* Sue Mosher, *Bayesian Spam Filters,* WINDOWS IT PRO, (Feb. 18, 2003), http://www.windowsitpro.com/article/exchange-server/bayesian-spam-filters.aspx. *See generally* THOMAS BAYES, AN ESSAY TOWARDS SOLVING A PROBLEM IN THE DOCTRINE OF CHANCES (1763), *reprinted in* PHILOSOPHICAL TRANSACTIONS 370, 370-418, *available at* http://rstl.royalsociety publishing.org/content/53/370.full.pdf+html.

[96] *See* Paul Graham, *Better Bayesian Filtering*, PAUL GRAHAM (Jan. 2003), http://paulgraham.com/better.html.

[97] *See generally* Stefanie Olsen, *One Man's Spam is Another's Art*, CNET NEWS, (July 26, 2006), http://news.cnet.com/One-mans-spam-is-anothers-art/2100-1025_3-6098479. html.

Supreme Court Justice Potter Stewart famously opined about pornography, "I shall not today attempt further to define the kinds of material I understand to be [hard-core pornography] . . . .[b]ut I know it when I see it," definitions of objectionable spam vary.[98] The United States Department of Education Institute of Education Services defines spam as "electronic junk mail or junk newsgroup postings. . . . [with s]ome people defin[ing] spam even more generally as *any* unsolicited e-mail."[99] Trend Micro, the vendor of the Mail Abuse Prevention System ("MAPS"), 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."[100]

Finally, the Office for Internet Safety provides a more general definition: "[s]pam refers to unwanted e-mail, usually of a commercial nature, sent out in bulk to an indiscriminate set of recipients."[101]

[28] Certain marketing organizations, like the Direct Marketing Association, do not provide a formal definition of spam, but rather

---

[98] Jacobellis v. Ohio, 378 U.S. 184, 197 (1964) (Stewart, J., concurring).

[99] *Weaving a Secure Web Around Education: A Guide to Technology Standards and Security*, NAT'L CENTER FOR EDUC. STAT., http://nces.ed.gov/pubs2003/secureweb/glossary.asp (last visited Jan. 18, 2011) (emphasis in original).

[100] Trend Micro, *Definition of Spam*, MAIL-ABUSE, http://www.mail-abuse.com/spam_def.html (last visited Jan. 18, 2011).

[101] *Jargon Buster*, *supra* note 1.

guidelines on responsible e-mail marketing.[102] Similarly, while some laws define spam directly,[103] others simply list permissible and prohibited activities.[104] Beyond the formal definitions, each user has his own idea of what constitutes unwanted "junk" e-mail.[105] While few definitions of spam include the act of making open relays available (as opposed to utilizing them), operators of vulnerable servers may also find themselves blocked by the same tools that seek out spammers.[106]

[29] With so many possible definitions of spam, it is little wonder that automated software-based tools cannot identify e-mail as spam in a way with which everyone, particularly the sender, may agree. Of notable controversy is how a software program determines whether a communication is "unsolicited."[107] Consider the situation where a professional attends a trade show and places his business card, which

---

[102] *See generally* Council for Responsible E-mail, *E-mail Delivery Best Practices for Marketers and List Owners,* DIRECT MARKETING ASS'N (Oct. 2005), http://www.the-dma.org/antispam/EmailBPFINAL.pdf.

[103] *E.g.*, 30 ILL. COMP. STAT. 500/25-70 (Ann. West 2009) (defining spam as "unsolicited electronic mail advertisements"); 815 ILL. COMP. STAT. 511/5 (Ann. West 2008) (extending the definition of spam to "any electronic mail advertisement that (i) is addressed to a recipient with whom the initiator does not have a prior or existing business or personal relationship and (ii) is not sent at the request of or with the express consent of the recipient").

[104] *See* Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003, Pub. L. No. 108-187, 117 Stat. 2699.

[105] *See* Carlton Vogt, *Spam: The Name's the Same, But We're Still Not Sure What It Means*, IT WORLD (Apr. 10, 2001), http://www.itworld.com/Man/2695/IWD010406 opethics/.

[106] *See id.* (discussing the need for a formal definition of spam, which allows the reader to draw the inference that without such a definition, some spammers will avoid the "spammer" tag and some non-spammers will be wrongfully labeled).

[107] *See generally* L. Pelletier et al., *Adaptive Filtering of SPAM* , U. ALA. BIRMINGHAM, 2 (2004), *available at* http://www.cis.uab.edu/zhang/Spam-mining-papers/Adaptive. Filtering.of.Spam.pdf.

identifies his e-mail address, into a drawing for a DVD player.[108] If the professional does not win the prize, but the vendor whose booth sponsored the drawing uses the e-mail address to send the professional information on the vendor's products, is that an unsolicited commercial message?[109] For that matter, is there a "prior or existing business or personal relationship" as required under the Illinois statutes?[110]

[30] The vendor likely may argue that willingly providing a business card containing an e-mail address in the context of a tradeshow booth represents consent to receive e-mail communications, since the vendor would not offer the DVD player without a reason (i.e. building a contact list).[111] But the professional may only have been interested in the DVD player, not the vendor's products, and he may not even remember having left a card in that particular vendor's booth. Thus, it would not be unexpected if the professional views the message as unwanted, and even unsolicited, and designates the message as spam.[112] This designation could promulgate further action, such as the professional or his ISP labeling the vendor as a spammer, which may then lead to the vendor's placement on multiple network block lists. Thus, it is possible that the opinion of a single individual or organization may block a sender's e-mail from reaching billions of users throughout the world.[113]

---

[108] *See* Terry Zink, *Does Handing Out Business Cards Constitute Opt-in?*, TERRY ZINK'S CYBER SECURITY BLOG, (Oct. 13, 2010, 9:32 AM), http://blogs.msdn.com/b/tzink/archive/2010/10/13/does-handing-out-business-cards-constitute-opt-in.aspx (suggesting that this situation implicates a separate category of "gray mail").

[109] *See id.*

[110] *See* 815 ILL. COMP. STAT. 511/5 (defining "unsolicited electronic mail advertisement"); *see also* 30 ILL. COMP. STAT. 500/25-70 (describing spam as "unsolicited electronic marl advertisements").

[111] *See* Zink, *supra* note 108.

[112] *See id.*

[113] *Cf.* Press Release, Cloudmark, Cloudmark Wants You to Show Us Your Spam in New Online Video Contest (June 22, 2010), *available at* http://www.cloudmark.com/en/press/releases/2010-06-22-cloudmark-wants-you-to-show-us-your-spam-in-new-online-video-contest (claiming that "Cloudmark solutions protect more than one billion

[31] Even when a user does not directly identify a message as spam, an automated filter operating on pre-existing rules and methods may improperly tag a non-commercial or solicited message as such.[114] If the initial message is not spam, blocking the sender's e-mails is essentially a false accusation with significant impact.

[32] Because messages scored as spam are typically kept from their intended destination (the recipient's inbox) and often routed to the deleted items or junk mail folder, or otherwise dumped in the "bit bucket,"[115] the sender may never know the recipient did not receive the message.[116] Also, the intended recipient may not always know which e-mail messages the spam filter routes away from his inbox, since, depending on the filter's configuration, the message may end up in his e-mail's spam or trash folder, or on his network or ISP mail server, to which he may not have access.[117] Moreover, even if the improperly blocked messages are on the

---

subscribers for the world's largest networks, including AT&T, Comcast, MySpace, NTT, Swisscom, and Time Warner Cable"); *Symantec Brightmail Message Filter,* SYMANTEC, http://www.symantec.com/business/brightmail-message-filter (last visited Jan. 17, 2011) ("Brightmail Message Filter protects over 800 million mailboxes and over 200 service providers globally."); *Frequently Asked Questions (FAQ), Spamhaus SBL,* SPAMHAUS, http://www.spamhaus.org/faq/answers.lasso?section=Spamhaus%20SBL#7 (last visited Jan. 17, 2011) [hereinafter *Spamhaus SBL*] (stating that "as of October 2009 the [Spamhaus Block List] user base exceeded 1,467,562,000 internet user mailboxes"). Because ISPs and network administrators often use multiple spam-blocking technologies, it is likely the number of protected computers overlap. *See* Justin Fielding, *Can Botnets Be Beaten?*, TECHREPUBLIC (Feb. 19, 2008), http://blogs.techrepublic.com.com/networking/index.php?cat=147&submit=view&paged=2. For example, both Spamhaus and Cloudmark block lists filter the author's Touro Law Center e-mail account.

[114] *See* Éloïse Gratton, *Dealing with Unsolicited Commercial Emails: A Global Perspective*, 7 J. INTERNET L. 3, 3 (2004).

[115] *See Bit Bucket*, CATB, http://www.catb.org/jargon/html/B/bit-bucket.html (last visited Jan. 16, 2011) (defining "bit bucket" as a computing term for the process of deleting unwanted information and noting the term might have come from the container into which the chads from computing punch cards are dropped).

[116] *See* Gratton, *supra* note 114.

[117] *See What Is a Spam Filter?,* WISEGEEK, http://www.wisegeek.com/what-is-a-spam-filter.htm (last visited Jan. 16, 2011).

recipient's computer, if he neglects to check the spam folder or empties the trash folder without reviewing the contents, he will remain unaware of the mistake.[118] In this way, even local false positives are problematic, particularly if the sender's identity, rather than the message's contents, cause the blocking.[119] Furthermore, if the false positive happens across a multi-network basis, both detection and remediation may be much more difficult.

VI. THE POTENTIAL IMPACT OF FALSE POSITIVES AND WRONGFUL LABELING

[33] For a casual e-mail exchange, a blocked message or account can be inconvenient. On the other hand, there may be times when e-mail receipt is mission-critical. A false positive from a spam filter or block list can make the difference between winning a bid for a government contract,[120] cause a litigant to miss a court-imposed pleadings deadline,[121] or otherwise cost time, money or both.

---

[118] *See What Is a False Positive?*, POPFILE, http://getpopfile.org/docs/glossary: falsepositive (last visited Jan. 26, 2011).

[119] *See id.*

[120] *See* GRAYSON COUNTY, TEX., INSTRUCTIONS FOR ELECTRONIC BID SUBMISSIONS, *available at* http://www.co.grayson.tx.us/Purchasing/PurchaseBidSub.htm (last visited Jan. 16, 2011); *see also* DEL. CODE ANN. tit. 29, § 6902(9) (2010) ("'Electronic bid' means the bidder . . . submits all documentation . . . only through an electronic process to an identified secure electronic mail account that will not be opened by the Office until the close of the bidding period. In this process, no hard copy documentation shall be submitted to the Office prior to the award of the contract.").

[121] *See, e.g.*, Eric Goldman, *"Spam Filter Ate My Electronic Filing Notice" Plaintiffs Get Another Chance* – Shuey v. Schwab, TECH. & MARKETING L. BLOG (Dec. 1, 2009, 10:15 AM), http://blog.ericgoldman.org/archives/2009/12/spam_filter_ate.htm (discussing an unpublished Third Circuit decision involving allegations of failing to receive a court's electronically filed order due to a spam filter); s*ee also* N.Y. ST. ATT'Y GEN., SERVICE ON THE OAG BY E-MAIL (2008), *available at* http://www.ag.ny.gov/serviceag_email.html (providing instructions for serving the Attorney General via e-mail under New York's Filing by Electronic Means pilot program); N.Y. ST. UNIFIED CT. SYSTEM, NEW YORK STATE COURTS E-FILING (NYSCEF), *available at* https://iapps.courts.state.ny.us/fbem/home.html (last visited Jan. 17, 2011) (permitting "the filing of legal papers by electronic means").

[34] In the commercial context, the risks can be both harder to quantify, but much greater in scope. Even the most zealous anti-spam advocates understand and acknowledge that a *solicited* commercial message may be proper.[122] Spamhaus clarifies the definition of spam, noting that "[s]pam is an issue about consent, not content. Whether the Unsolicited Bulk Email ("UBE") message is an advert, a scam, porn, a begging letter or an offer of a free lunch, the content is irrelevant - if the message was sent unsolicited and in bulk then the message is spam."[123]

[35] Although definitions sharply differ, most definitions of spam include some element of consent and/or solicitation.[124] Spamhaus, for example, indicates that a message is solicited when "the recipient has . . . verifiably granted deliberate, explicit, and still-revocable permission for it to be sent."[125] In contrast, the Direct Marketing Association provides a much broader view on consent. The Direct Marketing Association indicates that a recipient may provide affirmative consent to opt-in to receive commercial messages, or consent to opt-out of receiving commercial messages.[126]

[36] If a block list shared across users or ISPs generates a false positive, the false positive can keep a solicited message from reaching not only a single recipient, but also an entire list of recipients.[127] Consider an online

---

[122] *The Definition of Spam,* SPAMHAUS, http://www.spamhaus.org/definition.html (last visited Nov. 1, 2010).

[123] *Id.*

[124] *See, e.g.*, *id.*

[125] *See id.*

[126] *See Council for Responsible E-mail*, *supra* note 102, at 3 (identifying "double opt-in," "confirmed opt-in," and "opt-in" as forms of affirmative consent, and identifying "opt-out" as a form of consent). "Affirmative consent accompanied by clear and conspicuous notice provides a more highly qualified level of permission from recipients, which may help reduce the potential for spam complaints that could interfere with e-mail delivery." *Id.*

[127] *See, e.g.*, *Symantec Brightmail Message Filter*, *supra* note 113.

direct marketer that uses its own double opt-in list for its e-mail campaigns to ensure that it has affirmative consent for its messages.[128] Given the quality of its list and the nature of its mailings, the marketer typically enjoys a five percent average response rate to its direct e-mail solicitations.[129] Assume that, because a well-regarded block list incorrectly lists the marketer as a spammer, the ISPs for a significant number of users on the marketer's list block the marketer's e-mails.[130] This may result in a drastic drop in the solicitations response rate. Complicating the matter is the fact that if the messages are filtered rather than bounced back to the sender, the marketer's only indication that it is on a block list is the response rate, because it does not receive an external notice.[131] Further, even if some messages bounce back, the marketer may not have the tools or sophistication to properly measure and track the problem down to a particular set of ISPs or block list(s).[132]

[37] The above hypothetical is not limited to direct marketers. The Interactive Advertising Bureau ("IAB") has published an entire guide to e-mail deliverability, which states that "[m]ore than 20% of legitimate marketing messages are incorrectly identified as spam by server and client

---

[128] *See Council for Responsible E-mail*, *supra* note 102, at 3. Double opt-in occurs when "[a] user has elected to receive e-mail newsletters or stand alone commercial messages. A confirmation e-mail is then sent to the user to which he/she must reply . . . before the list owner may add [him/her] to [his] list." *Id.*

[129] *How Can We Increase Our Email Marketing Response Rates?*, DESTINATIONCRM.COM (Dec. 9, 2002), http://www.destinationcrm.com/articles/default.asp?ArticleID=2714 (stating that response rates to e-mail campaigns have been reported as ranging anywhere from one to two percent to as high as twenty-five percent).

[130] *See* Roderick Suganob, *Spam Filters Do Generate False Positive*, ASSOCIATED CONTENT, (May 17. 2007), http://www.associatedcontent.com/article/249172/spam_filters?cat=35 (providing a parallel discussion about the issue of false positives and the relationship between spam filters and marketers).

[131] *See id.*

[132] *See id.*

level spam filtering, so chances are that if you aren't watching it closely then you have deliverability problems."[133]

[38] The IAB suggests multiple methods for evaluating and dealing with deliverability problems, including bounce reports, monitoring of e-mail abuse discussion lists and careful review of data collection methods.[134] Given that the IAB's members are among the larger, more-established (and therefore legally exposed) marketers, 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, emphasizing that the problems companies face with respect to filters, block lists and e-mail non-delivery are truly great.[135]

VII. REMEDYING IMPROPER LISTING: THE LIMITS OF THE SELF-REGULATORY APPROACH

[39] Given the Internet's tradition of collaborative self-regulation, it would seem appropriate that, in the event a sender is falsely designated as a spammer, he should be able to remedy the situation without turning to the courts.[136] To address false positives from a user's filter, many senders include explicit instructions for recipients to add the sender to a

---

[133] *Marketer & Agency Guide to Email Deliverability*, INTERACTIVE ADVERTISING BUREAU, 3 (2006), http://www.iab.net/emaildeliverability; *see also The IAB Releases an Industry Guide to Email Deliverability*, INTERACTIVE ADVERTISING BUREAU (OCT. 16, 2006), http://www.iab.net/about_the_iab/recent_press_releases/press_release_archive/press_release/5086.

[134] *See id.* at 8-12.

[135] *General Members*, INTERACTIVE ADVERTISING BUREAU, http://www.iab.net/member_center/1521/1534 (last visited Jan. 17, 2011) (displaying a members list that includes Time Inc., Disney Interactive Media Group, and New York Times Digital).

[136] *See* JULIAN DIBBELL, MY TINY LIFE: CRIME AND PASSION IN A VIRTUAL WORLD 11-28 (1998), *available at* http://www.lulu.com/items/volume_63/1070000/1070691/3/print/1070691.pdf (recounting how an online virtual community created "law" and "punishment" to respond to a member's violation of the common social norm).

"whitelist," that is, a list of approved e-mailers.[137] But this process may not be easy for some users, as it requires their affirmative act.[138] Further, in light of the vast number of different software and ISP combinations through which users receive e-mail,[139] senders may find this approach less than successful.[140] The whitelist approach also has the weakness of applying only to single users' e-mail accounts or his personal spam filtering setup, rather than a large number of potential recipients.[141]

[40] A more scalable approach involves obtaining placement on a large ISP's whitelist, with the hope that those users depending on the ISP to block spam will benefit from the ISP's "blessing" of the sender.[142] While this approach is more efficient than relying upon an individual's whitelist, it still requires a multi-step process, in which the sender likely identifies those ISPs whose users represent significant percentages of the sender's

---

[137] *See Glossary*, SINGAPORE SPAM CONTROL RESOURCE CENTRE, http://www.spamcontrol.org.sg/glossary.html (last visited Jan. 20, 2011) (defining a whitelist as the "[t]he opposite of a blacklist," or a list of "'good' senders, so that all the e-mails from [those senders] will be accepted"); *Newsletter*, GUIDESTAR.ORG (Aug. 2006), http://www.guidestar.org/news/newsletter/archive/aug_2006.jsp ("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 whitelist, or mail system whitelist. Adding the address will help ensure that you receive the Newsletter and that your e-mail software displays HTML and images properly.").

[138] *See* SINGAPORE SPAM CONTROL RESOURCE CENTRE, *supra* note 137.

[139] *See How To Make Sure Listeners Receive Your Email*, PROMOSUITE INTERACTIVE, http://www.listeneremail.com/email/emailhelp.htm (last updated Sept. 12, 2007).

[140] *See* Press Release, *Loren McDonald,* NetlinkBlue, How To Get on a Whitelist, *available at* http://www.netlinkblue.com/how-to-Get-Whitelist.asp (last visited Jan. 21, 2011) ("You probably have a line in your email message near the top, asking the recipient to add your sending address to his or her address book or contact/safe-sender list. But, that's almost too late in the process.").

[141] *See* Matt Garrett, *How E-mail Whitelists Work,* ANTI SPAM FOR OUTLOOK, http://antispamforoutlook.net/a80939-hoe-e-mail-whitelists-work.cfm (last visited Nov. 2, 2010).

[142] *See* Stefan Pollard, *Whitelisting: A Privilege Worth Earning*, CLICKZ (May 9, 2007), http://www.clickz.com/clickz/column/1698446/whitelisting-a-privilege-worth-earning.

mailing list, researches and complies with any ISP whitelist procedures, and finally secures placement on the whitelist.[143]

[41] But, not every ISP maintains complete control over its global whitelist; some leave the process in the hands of the users.[144] Even under these ISP whitelist procedures, senders may faces significant procedural burdens. AOL's white list process includes technical, formatting and procedural and policy requirements, including security obligations on the sender's own mail server.[145] For an e-mail marketer, keeping up with these separate requirements can be extremely onerous.[146] In fact, companies may not even consider the issue of whitelisting before becoming subject to blocking. In either event, the whitelisting process is imperfect, and companies, whether by mistake, or through critics' or competitors' malice, may still end up on block lists.[147]

[42] Another approach is to obtain third-party certification as a non-spammer.[148] For example, Return Path offers a commercial certification service, with pricing ranging from $440 to $82,500 annually for commercial mailers, depending on their monthly e-mail volume.[149] The

---

[143] *See* McDonald, *supra* note 140.

[144] *See Selecting Your Level of Spam Protection*, EARTHLINK, www.earthlink.net/webmail/help/earthlink/en_US/spamblocker/protection.html (last visited Jan. 20, 2011).

[145] *See Conditions for Gaining Whitelisted Status*, AOL POSTMASTER, http://postmaster.aol.com/cgi-bin/whitelist/whitelist_guides.pl (last visited Oct. 28, 2010).

[146] *See id.*

[147] *See* Stefanie Olsen, *Are Spam 'Blocklists' Going Too Far?*, ZDNET (July 15, 2002), http://m.zdnet.com.au/are-apam-blocklists-going-too-far-120266689.htm.

[148] *See* Vincent Schiavone et al., *Trusted Email Open Standard, A Comprehensive Policy and Technology Proposal for Email Reform*, ePRIVACY GROUP, 13, 17 (May 2003), http://www.ftc.gov/bcp/workshops/spam/Supplements/eprivacygp.pdf.

[149] *Great Value/High ROI, Reach More Subscribers with Richer Content*, RETURN PATH, http://www.returnpath.net/commercialsender/certification/pricing/ (last visited Jan. 16, 2011).

requirements for this service are rather detailed,[150] and the applicability, though widespread, is far from universal.[151] Here too, many e-mailers may be unaware of the existence of third-party whitelisting, and for some, the costs or efforts of compliance may seem too great, particularly when they are not involved with direct e-mail marketing.

[43] The most efficient approach for a sender improperly included on a block list or a spam filter is to request removal directly from that list or filter.[152] The first significant challenge is to verify that the sender is in fact on that block list or filter.[153] But this task is not always as simple as it sounds, because while some operators, such as Spamhaus, make their block lists public, others do not.[154] A sender on a closed list may only suspect it is there based on inference, examining which ISPs appear to block the sender's mail, and then attempting to determine what spam filter

---

[150] *See generally Minimum Standards & Requirements for the Return Path Certification Shared IP Program*, RETURN PATH, http://www.returnpath.net/commercialsender/certification/lib/documents/SharedIPsMinimumStandardsandRequirements.pdf (last visited Jan. 21, 2011).

[151] *See* Bus. Wire, *Return Path Re-Launches the Bonded Sender Program with More Rigorous Standards and New Name*, *Sender Score Certified*, FIND ARTICLES (Apr. 18, 2006), http://findarticles.com/p/articles/mi_m0EIN/is_2006_April_18/ai_n26832534/ ("Sender Score Certified is the industry's leading accreditation system, used by more than 35,000 receiving domains, including MSN Hotmail, Windows Live Mail Beta and Roadrunner, covering more than 250 million email mailboxes worldwide.").

[152] *See* Web Marketing Today, *Spam Blacklist Removal*, WILSON WEB, http://www.wilsonweb.com/05/020529b.htm (last visited Jan. 21, 2011).

[153] *See* Trend Micro, *IP Address Removal Process,* MAIL-ABUSE, http://www.mail-abuse.com/removereq.html (last visited Jan. 21, 2011).

[154] *See generally Blocklist Removal Center,* SPAMHAUS, http://www.spamhaus.org/lookup.lasso (last visited Jan. 21, 2011). In contrast, Brightmail is a "black box"-type system, in which all e-mail goes in one end and spam-free e-mail comes out the other end. *See generally Data Sheet: Messaging Security, Symantec Brightmail Gateway,* SYMANTEC, http://eval.symantec.com/mktginfo/enterprise/fact_sheets/b-symc_brightmail_gateway_DS_20012004-1.en-us.pdf (last visited Jan. 16, 2011).

or block list the ISPs may have in common.[155] This, however, is an inexact method and may not be determinative, especially if the ISPs use multiple lists and filters to ensure complete coverage.[156] A sender may have to make a best guess, investigate all possible lists and filters, and then pursue removal options.[157]

[44] Yet even when a sender determines which block lists or filters affect its messages, removal is far from certain, particularly in light of the challenges regarding the various definitions of spam.[158] As previously discussed, spam for one party may be appropriate e-mail marketing for another.[159] Furthermore, a sender may consider single opt-in or even opt-out sufficient to prevent against the perception of spam, but block lists may deem anything other than double (or verified) opt-in as spam, and block the sender's messages.[160]

---

[155] *See generally Blacklists: Major Blocks on the Path to the Inbox,* G-LOCK SOFTWARE (Oct. 7, 2009), http://www.glockeasymail.com/blacklists-blocks-path-to-inbox/.

[156] *See* William K. Cole, *Blacklists, Blocklists, DNSBL's, and Survival: How To Survive as a Non-combatant Emailer in the Spam Wars,* SOLID CLUES CONSULTING, http://www.scconsult.com/bill/dnsblhelp.html (last visited Nov. 3, 2010) ("Some [Mail Transfer Agents, such as ISPs] use multiple DNSBL's, weighted scoring, and other techniques to decide whether to accept a piece of mail.").

[157] *See Blacklists: Major Blocks on the Path to the Inbox*, *supra* note 155.

[158] *See supra* notes 97-106 and accompanying text.

[159] *See* Cohn & Newitz, *supra* note 52; *see also supra* notes 97-106 and accompanying text.

[160] *See* Daniel Owen, *An Application Agnostic Review of Current Spam Filtering Techniques*, DANIELOWEN.COM, 4 (Aug. 27, 2007), http://www.danielowen.com/agnostic_spam. In some circumstances, senders may take comfort in compliance with applicable laws such as CAN-SPAM, even though the block list providers dismiss the standards of such laws as insufficient. *See* Steve Linford, *United States Set To Legalize Spamming on January 1, 2004*, SPAMHAUS (Nov. 22, 2003), http://www.spamhaus.org/news.lasso?article=150 (describing how the CAN-SPAM Act "legalizes spamming instead of banning it").

[45] The next step is to determine the most appropriate method for removal. Some block lists and filters provide a removal process (and even contact senders regarding their removal from the list),[161] but, because the fight against spam is never-ending battle, a sender's claim for removal may face a presumption of invalidity.[162] This presumption stems from the negative views levied against spammers, and leads to the vicious reality that claims of wrongful inclusion on block lists are likely to fall on deaf ears.[163]

[46] The view against spam is so strong, that if a third party sends unauthorized spam on behalf of a marketer, the marketer, because it has benefited from the transmission, may receive the dubious title of spammer.[164] In fact, some lists will not even accept communications or proposed evidence from accused or suspected spammers, rather the ISPs with which the accused work must argue on their behalf.[165] Moreover, if the ISP is unwilling or unable to assist, or if the accused cannot otherwise move the ISP to take action, the accused may face the dilemma of possibly remaining on the block list or filter indefinitely, or switching ISPs, which raises suspicion among anti-spam advocates.

[47] In light of the severe consequences senders face as a result of having their e-mail messages blocked across numerous ISPs and networks, it is no surprise that many accused spammers retain attorneys to advocate on their behalf. Of concern is the possibility that block list and filter

---

[161] *See* NJABL.ORG, http://njabl.org/remove.html (last visited Jan. 16, 2011) (instructing spammers on how to remove themselves from the Not Just Another Bogus List block list).

[162] *See generally Road Runner Mail Blocks,* ROAD RUNNER, http://security.rr.com/mail_blocks.htm (last visited Jan. 16, 2011).

[163] *See ROKSO FAQ, supra* note 3 ("Spammers are not people known for honesty; in fact they are almost all con men, fraudsters and chronic liars.").

[164] *See* Alongi, *supra* note 57 ("Using prohibited spamming techniques to promote a business is not allowed even if the business uses a third party spammer to send e-mail on its behalf.").

[165] *See generally Road Runner Mail Blocks*, *supra* note 162.

operators may view such action negatively, believing that any sender utilizing an attorney to press its case is an actual spammer using unfounded legal threats to coerce removal from a list on which it properly belongs.[166] Further, even if a block list or filter operator entertains communication from an attorney on behalf of a sender, the operator is likely under no obligation to act, and may nevertheless elect not to remove the sender from its lists.

VIII. LITIGATION AS A REMEDY: CLAIMS, EXISTING CASES AND EVOLVING DOCTRINE

[48] If a sender believes it is wrongfully included on a block list or within a spam filter, but is unable to obtain removal after exhausting all self-help processes and remedies, what are the sender's remaining options? Under United States law, senders have turned to the courts for redress, requesting equitable relief, monetary damages, or both.[167] A sender's strongest (potential) claims are defamation and intentional interference with prospective business relationships.[168] And, while the courts, cases and claims vary, one almost universal defense block list and filter operators invoke against a sender's claim is the 47 U.S.C. § 230 safe harbor.[169]

---

[166] *See ROKSO FAQ*, *supra* note 3 ("Spamhaus regularly receives letters from spammer's [sic] lawyers attempting to claim that all of a spammers [sic] records are in error and demanding all therefore be removed. [Spamhaus] naturally pay[s] little attention to such requests.").

[167] *See* discussion *infra* Part VIII.B.

[168] *See infra* Part VIII.A. The following analysis presupposes that a sender listed on a block list is not a spammer.

[169] *See* 47 U.S.C. § 230 (2006).

A. Wrongful Inclusion on Block Lists or Filters: The Elements of Potential Claims

1. Defamation

[49] The Internet community is not alone in its negative view of spamming.[170] In fact, spamming is a crime in a number of jurisdictions.[171] Accordingly, a false designation on a block list carries the potential to serve as an accusation of a crime.[172]

[50] The Restatement (Second) of Torts provides:

> 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. [173]

Defamation is available 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

---

[170] *See* Mail Abuse Prevention Sys. LLC v. Black Ice Software, Inc., No. CV 788630, 2000 WL 34016435, at *7 (Cal. Super. Ct. Oct. 13, 2000) ("'Spammer' and 'spam' are disparaging labels in the Internet business community.").

[171] *E.g.*, VA. CODE ANN. § 18.2-152.3:1 (Supp. 2010).

[172] *See* RESTATEMENT (SECOND) OF TORTS § 558 (1977).

[173] *Id.*

> (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.[174]

[51] Comments (d) and (e) to Section 569 of the Restatement (Second) of Torts provide that publishing an accusation of a crime that can result in imprisonment, or a statement that damages the subject's ability to do its business, is actionable per se without need to show special damages.[175] Thus, when a sender is wrongfully block listed, filtered or otherwise identified as a spammer to potential service providers and customers, and the block list and filter operator has done so either negligently or maliciously, the sender may have an action in defamation.[176]

2. Intentional Interference with Prospective Business Relationships

[52] A major element common to all spam definitions is that the bulk messages are commercial in nature.[177] Thus, it follows that when a block list or filter operator prevents an alleged spammer's messages from reaching their recipients, the operator's intention, in part, is to deny the spammer the commercial opportunities the messages represent.[178] As such, a non-spammer wrongfully block listed or filtered, may look to the

---

[174] RESTATEMENT (SECOND) OF TORTS § 561 (1977).

[175] RESTATEMENT (SECOND) OF TORTS § 569 cmt. d, e (1977); *see also* Candace Rondeaux, *Anti-Spam Conviction Is Upheld, N.C. Man Flooded AOL Customers with Unsolicited E-Mail*, WASH. POST, Sept. 6, 2006, at B3, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2006/09/05/AR2006090501166.html (discussing the conviction of Jeremy Jaynes and his nine-year prison sentence).

[176] *See* RESTATEMENT (SECOND) OF TORTS §§ 558, 561 (1977).

[177] *See* discussion *supra* Part V.

[178] *See* Sharon Gaudin, *Q & A: Dave Rand on Spam*, NETWORK WORLD (Sept. 10, 2001), http://www.networkworld.com/research/2001/0910featside4.html. "MAPS is not about stopping spam. MAPS is about stopping spammers. . . . It's clear that the MAPS lists can help reduce the amount of spam that subscribers get, but they also help to reduce the number of spammers." *Id.* (quote provided by David Rand, Executive Director, Mail Abuse Prevention Systems).

tort of intentional interference with prospective contractual relation for remedy:

> One who intentionally and improperly interferes with another's prospective contractual relation . . . 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.[179]

[53] The cause of action of intentional interference with prospective contractual relation is even more applicable in situations where block list and filter operators *publicly* identify an alleged spammer or label its messages as "spam," or automatically place the sender's messages in a recipient's junk or deleted mail folder. In such situations, it is clear that the operator's intention is to keep the sender from doing business with the operator's user base.[180] This intention is further evident where an operator labels not only bulk messages, but all of a sender's messages, as spam, which greatly impedes the sender's ability to operate its business at all.[181]

---

[179] RESTATEMENT (SECOND) OF TORTS § 766B (1979).

[180] *See* Gaudin, *supra* note 178.

[181] *See* Sharon Gaudin & Suzanne Gaspar, *The Spam Police*, NETWORK WORLD (Sept. 10 2001), http://www.networkworld.com/research/2001/0910feat.html ("Ron May, MIS manager for SearsCarpet.com, a franchise carpet and upholstery cleaning service in Columbus, Ohio, knows all about collateral damage. May says 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.").

3. Other Possible Claims

[54] A sender wrongfully labeled a spammer has avenues of recourse beyond claims for defamation and intentional interference with prospective contractual relation. Depending on the facts and applicable state law, a plaintiff also may consider claims of unfair competition, restraint of trade, and interference with contractual relations.[182] The difficulty with such claims, though, is that while a sender may demonstrate actual damages – to the extent that a blocked communication caused the party specific harm[183] – the specter of 47 U.S.C. § 230's broad immunity often impedes plaintiffs from receiving any or all of their sought after redress.[184]

B. Spam Filter Litigation in United States Courts

[55] United States courts litigate a number of cases regarding wrongful operation of spam filters. Some cases focus on the First Amendment right to free speech,[185] while others follow the business tort pattern previously

---

[182] *See* Kramer v. Perez, 595 F.3d 825, 828 n.4 (8th Cir. 2010) (noting that the plaintiff brought multiple claims, including "unfair competition, conversion, trespass, unjust enrichment, intentional interference with contract, and intentional interference with prospective business advantage"); Optinrealbig.com, LLC v. Ironport Sys., Inc., 323 F. Supp. 2d 1037, 1048 (N.D. Cal. 2004) (noting that the plaintiff sought injunction based on claims of "trade libel, intentional interference with contractual relations and unfair competition"); Mail Abuse Prevention Sys. LLC v. Black Ice Software, Inc., No. CV 788630, 2000 WL 34016435, at *1 (Cal. Super. Ct. Oct. 13, 2000) (noting that the cross-complainant filed claims of, "(1) defamation; (2) intentional interference with contractual relationship; (3) intentional interference with prospective economic advantage; (4) unfair competition; and (5) restraint of trade").

[183] *See* e360 Insight, LLC v. Spamhaus Project, No. 06 C 3958, 2010 U.S. Dist. LEXIS 57654, at *22-25 (N.D. Ill. June 11, 2010).

[184] S*ee* 47 U.S.C. § 230(c) (2006); *see also* Zango, Inc. v. Kaspersky Lab, Inc., 568 F.3d 1169, 1173-74 (9th Cir. 2009).

[185] *See* Cyber Promotions, Inc. v. Am. Online, Inc., 948 F. Supp. 436, 447 (E.D. Pa. 1996) (holding that America Online was not dedicated to public use; therefore, First Amendment protections did not extend to Cyber Promotions' marketing materials); *see also* White Buffalo Ventures, LLC v. Univ. of Tex., 420 F.3d 366, 368-69 (5th Cir. 2005)

discussed.[186] However, as the following sections reveal, regardless of the type of claim, 47 U.S.C. § 230 largely limits the success of most spam filter litigation.

1. The *Black Ice and OptInRealBig* Cases: Early Exploration of the Limits of 47 U.S.C. § 230(c)(2)(B)

[56] A number of defendants in cases concerning spam filters and similar technologies raise 47 U.S.C. § 230(c)(2) as a defense.[187] The first provision of 47 U.S.C. § 230(c)(2) provides immunity for both users and providers of an "interactive computer service" who, in "good faith," limit access to a broadly defined list of "objectionable" material.[188] The second provision protects those who provide a technical means of access to the material.[189] The first cases invoking this statute involved similar free speech concerns to the *Stratton Oakmont* case, namely the use of message boards and other textual postings.[190]

[57] *Mail Abuse Prevention Systems LLC v. v. Black Ice Software, Inc.,* provides an early example of spam filter litigation.[191] Mail Abuse

(rejecting White Buffalo's argument that a state university's use of spam filters violated its First Amendment rights).

[186] *See, e.g.*, *Black Ice*, 2000 WL 34016435, at *1.

[187] *See* Zango, Inc. v. Kaspersky Lab, Inc., 568 F.3d 1169, 1173-74 (9th Cir. 2009); *see also* 47 U.S.C. § 230(c) (2006).

[188] *See* 47 U.S.C. § 230(c)(2).

[189] *See id.*

[190] *See, e.g.*, Zeran v. Am. Online, Inc., 129 F.3d 327, 328, 332 (4th Cir. 1997) (holding America Online not liable for defamatory postings on one of its message boards); *see also* Blumenthal v. Drudge, 992 F. Supp. 44, 49-50 (D.D.C. 1998) (holding America Online immune from liability for making available to its subscribers a defamatory article written by third-party columnist). *See generally* Stratton Oakmont, Inc. v. Prodigy Services Co., No. 31063/94, 1995 N.Y. Misc. LEXIS 229 (N.Y. Sup. Ct. May 24, 1995).

[191] *See* Mail Abuse Prevention Sys. LLC v. Black Ice Software, Inc., No. CV 788630, 2000 WL 34016435, at *1 (Cal. Super. Ct. Oct. 13, 2000)

Prevention System ("MAPS") operated spam filter services and identified Black Ice as a spammer in its "Realtime Blackhole List."[192] Shortly thereafter, MAPS commenced legal action against Black Ice under California's Business & Professions Code, §17538.45, the state anti-spam law.[193] In response, "Black Ice filed [a] Cross-Complaint alleging: (1) defamation; (2) intentional interference with contractual relationship; (3) intentional interference with prospective economic advantage; (4) unfair competition; and (5) restraint of trade."[194]

[58] MAPS' raised 47 U.S.C. § 230(c) as a complete defense to Black Ice's counterclaims.[195] The court analyzed MAPS' status as an interactive

---

[192] *Id.*

[193] *Id.* Section 17538.45 of California's Business & Professional Code states:

> (b) No registered user of an electronic mail service provider shall use or cause to be used that electronic mail service provider's equipment located in this state in violation of that electronic mail service provider's policy prohibiting or restricting the use of its service or equipment for the initiation of unsolicited electronic mail advertisements.
> (c) No individual, corporation, or other entity shall use or cause to be used, by initiating an unsolicited electronic mail advertisement, an electronic mail service provider's equipment located in this state in violation of that electronic mail service provider's policy prohibiting or restricting the use of its equipment to deliver unsolicited electronic mail advertisements to its registered users.

CAL. BUS. & PROF. CODE ANN. § 17538.45 (West 2008).

[194] *Black Ice*, 2000 WL 34016435, at *1. In addition to the litigation involving Black Ice Software, MAPS also was involved in litigation with Media3, Yesmail, Experian (formerly Exactis), and Harris Interactive. *See* Media3 Tech., LLC v. Mail Abuse Prevention Sys., LLC, No. 00-CV-12524-MEL, 2001 WL 92389 (D. Mass. Jan. 2, 2001); Suzanne Gaspar, *E-mail Marketer Settles Suit Against MAPS*, NETWORK WORLD (Oct. 26, 2001), http://www.networkworld.com/news/2001/1026maps.html; Press Release, Harris Interactive, Harris Interactive Files Suit Against AOL, Microsoft, Qwest and Other ISPs Over Restraint of Trade (July 31, 2000), *available at* http://www.dotcomeon.com/harris.html; Oscar S. Cisneros, *Yesmail Fights Blacklist Threat*, WIRED (July 18, 2000), http://www.wired. com/politics/law/news/2000/07/37621.

[195] *Black Ice*, 2000 WL 34016435, at *8.

service provider (since it did not provide e-mail services directly), and found that MAPS had standing under § 230(c)(2)(B) as an "access software provider [that] helps enable other computer users accessing the Internet."[196] Next, the court analyzed "whether spam is 'harassing' or 'otherwise objectionable' material under § 230(c)(2)(A)."[197] The court found that spam could qualify as such material, but noted that MAPS also blocked other messages, not merely the alleged objectionable spam.[198] Thus, the court found standing for Black Ice's counterclaims.[199]

[59] Black Ice's defamation claim focused on the publication of Black Ice's name in MAPS' Realtime Blackhole List.[200] MAPS referred to Black Ice as a spammer, a statement for which California defamation law does not require pleading actual damages.[201] According to the court's analysis of § 230(c)(2)(B), listing Black Ice as a spammer was not merely a technical enabling of spam blocking, but an "announcement," which was a separate act.[202] Thus, the defamation claim was allowed to stand.[203] The court also found standing for Black Ice's intentional interference with prospective economic advantage, unfair competition and restraint of trade, and punitive damages claims, but it rejected Black Ice's claim for intentional interference with contractual relations because Black Ice failed

---

[196] *Id.*

[197] *Id.* at *9.

[198] *See id.*

[199] *Black Ice*, 2000 WL 34016435, at *10.

[200] *See id.* at *7.

[201] *Id.* at *7 ("[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.").

[202] *Id*. at *10.

[203] *Id.*

to allege "what services were contracted for, or how [they were] disrupted."[204]

[60] *Black Ice* contrasts sharply with *OptInRealBig.com v. Ironport Systems.*[205] In *OptInRealBig*, the plaintiff, a direct e-mail marketer, sued Ironport because an Ironport subsidiary, Spamcop.net, reported OptInRealBig as a spammer to OptInRealBig's ISPs.[206] Unlike MAPS, Spamcop operated by passing along complaints from recipients of alleged spam to the apparent sender's ISP.[207] Given that Spamcop acted as an interactive service provider and merely passed along reports of spamming in accordance with the definition of 47 U.S.C. § 230(c)(1), the court found that the statute fully protected Spamcop/Ironport from liability.[208] Even after upholding Ironport's immunity under § 230, the court went on to analyze and reject OptInRealBig's claims regarding trade libel, interference with contractual relations, and unfair business practices.[209]

2. *Zango v. Kaspersky Lab* and the Evolving Understanding of "Interactive Service Provider" and "Good Faith"

[61] The interpretation of 47 U.S.C. § 230 continues to evolve, with most courts relying on subsection (c)(1) to reject liability claims against web site owners for third-party content, in contexts as broad as search engines,[210] online business listing categories, [211] and consumer reviews.[212]

---

[204] *Black Ice*, 2000 WL 34016435, at *10-12.

[205] *See generally* Optinrealbig.com, LLC v. Ironport Sys., Inc., 323 F. Supp. 2d 1037 (N.D. Cal. 2004).

[206] *Id.* at 1039.

[207] *Id.*

[208] *Id.* at 1044, 1052.

[209] *Id.* at 1048-50.

[210] *See, e.g.*, Parker v. Google, Inc., 422 F. Supp. 2d 492, 500-01 (E.D. Pa. 2006) (holding Google not liabile for third party USENET postings it archived for public viewing).

In fact, it appears that section 230(c)(1) protection only fails when the site owner is an "interactive service provider" *and* the "information content provider" for the material upon which the case is based.[213] Instead, section 230(c)(1) protects interactive service providers from "information provided by *another* information content provider."[214] But, as Eric Goldman notes, subsection (2) of § 230(c) "doesn't get much love," as evidenced by the facts that it is not specifically referenced in the Code's legislative history, it has been used to resolve fewer than twelve cases, and it has been "effectively ignored in academic literature."[215]

[62] While 47 U.S.C. § 230(c)(2)(A) appears to address an ISP's spam filtering on behalf of its users, it is unclear from the statute's plain language whether it also covers spam block list operators, at least those whose lists are available online.[216] The Ninth Circuit recently addressed a related question in *Zango v. Kaspersky Lab, Inc.*, in which a creator and

---

[211] *See, e.g.*, Prickett v. InfoUSA, Inc., 561 F. Supp. 2d 646, 652 (E.D. Tex. 2006) (holding infoUSA not liable to individuals it mistakenly listed as adult businesses).

[212] *See, e.g.*, Nemet Chevrolet, Ltd. v. Consumeraffairs.com, Inc., 564 F. Supp. 2d 544, 555 (E.D. Va. 2008) (rejecting the claims of an automobile dealer that sued a website for posting consumers' opinions).

[213] *See, e.g.*, Carafano v. Metrosplash.com, Inc., 339 F.3d 1119, 1122 (9th Cir. 2003) ("Through [47 U.S.C. § 230(c)(1)], Congress granted most Internet services immunity from liability for publishing false or defamatory material so long as the information was provided by another party."); *see also* 800-JR Cigar, Inc. v. Goto.com, Inc., 437 F. Supp. 2d 273, 295 (D.N.J. 2006) ("Immunity does not seem to fit here because the alleged fraud is the use of the trademark name in the bidding process, and not solely the information from third parties that appears on the search results page. It is not the purpose of the Act to shield entities from claims of fraud and abuse arising from their own pay-for-priority advertising business, rather than from the actions of third parties.").

[214] 47 U.S.C. § 230(c)(1) (2006) (emphasis added).

[215] Eric Goldman, *47 U.S.C. 230(c)(2) and Immunity for Online Filtering*, ERIC GOLDMAN, http://www.ericgoldman.org/Speeches/47usc230c2.pdf (last visited Jan. 17, 2011).

[216] *See* 47 U.S.C. § 230(c)(1)(A). *See generally* Zango, Inc. v. Kaspersky Lab, Inc., 568 F.3d 1169 (9th Cir. 2009).

distributor of advertising-driven online games and video catalogs sued the owner of a software product that filtered the plaintiff's software as "malware."[217] The district court, applying § 230(c)(2)(B), dismissed the plaintiff's various business tort claims, and the Ninth Circuit affirmed on appeal.[218]

[63] In affirming the district court's ruling, the court upheld the determination that Kaspersky was an "interactive computer service,"[219] declining Zango's argument that the definition covers only services that "enables people to access the Internet or access content found on the Internet."[220] Following this determination, the court rejected Zango's

---

[217] *Zango*, 568 F.3d at 1170-72. The court noted:

> [Kaspersky's] software helps filter and block unwanted malicious software, known as "malware," that can compromise the security and functionality of a computer. . . .
>
> The Kaspersky software classifies Zango's programs as adware, a type of malware. Once installed on a user's computer, adware monitors a user's Internet browsing habits and causes "pop-up ads" to appear on a computer screen while the user browses the Internet. Adware can also open links to websites and computer servers that host malware and expose users' computers to infection, and can swamp a computer's memory and slow down computer speed and performance. For these reasons, pop-up ads and adware are unpopular among computer users, and consumers often install security software specifically to block adware.

Id. at 1171.

[218] *See id.* at 1172, 1177-78. Throughout its opinion, the Ninth Circuit analyzed both the legislative history and judicial interpretation of 47 U.S.C. §230, and noted that while it applied §230(c)(2) in the present case, previous cases had primarily focused on §230(C)(1). *See generally id.* The court rejected the plaintiff's reliance on a footnote in an earlier case, *Batzel v. Smith*, referencing (c)(2), because the provision had been "not relevant" to the actual decision in *Batzel*. *Id.* at 1175 (citing Batzel v. Smith, 33 F.3d 1018, 1030 n.14 (8th Cir. 1994)).

[219] *Id.* at 1175 ("We agree with the district court that Kaspersky is a 'provider' of an 'interactive computer service' under the plain terms of § 230(c).").

[220] *Id.*

effort to read an implied "good faith" standard into 230(c)(2)(B) – an argument Zango failed to raise in district court – and observed "that subparagraph (B) comes with only one constraint: the protection afforded extends only to providers who 'enable or make available to . . . others' the technical means to restrict access to material that either the user *or* the provider deems objectionable."[221]

[64] Zango also argued that since Kaspersky made the decision as to which software to block, Kaspersky did more than merely make the technical means to restrict access available, because the users were not given control over restriction.[222] The court rejected this argument, stating:

> By providing its anti-malware software and malware definition update services, Kaspersky both enables and makes available the technical means to restrict access to malware. Users choose to purchase, install, and utilize the Kaspersky software. Regardless of whether Zango is correct in its allegation that Kaspersky does not provide users of Kaspersky products a choice to override the security software and download and use Zango, there is no question that Kaspersky has "made available" for its users the technical means to restrict access to items that Kaspersky has defined as malware. Therefore, Kaspersky satisfies the requirements of subsection (B) so long as the blocked items are objectionable material under § 230(c)(2)(A).[223]

The court assumed that users could choose whether to install and utilize the Kaspersky software, and that this ability "is consistent with the statute's express policy of relying on the market for the development of interactive computer services."[224]

---

[221] *Zango*, 568 F.3d at 1177 (alterations in original).

[222] *Id.* at 1176.

[223] *Id.*

[224] *Id.* at 1177.

3. *e360 v. Spamhaus*: Jurisdictional Issues in International Block Lists

[65] A recent, and controversial, case regarding spam block lists and alleged false listings involves e360 Insight ("e360"), an online marketer, and its placement on the Spamhaus ROKSO list.[225] Located in Wheeling, Illinois, e360 first brought suit against Spamhaus in June 2006 in the Illinois Circuit Court alleging that Spamhaus had improperly listed e360 on the ROKSO list even though e360 denied having been a spammer or otherwise qualify for the ROKSO list.[226] After e360 obtained a temporary restraining order from the Illinois state court, Spamhaus requested, and received, removal of the case to the U.S. District Court for the Northern District of Illinois.[227] After the case was moved to the District Court, Spamhaus denied that the court had jurisdiction, and shortly thereafter its attorney's withdrew.[228] On September 13, 2006, the

[225] *See* e360 Insight, LLC v. Spamhaus Project, No. 06 C 3958, 2010 WL 2403054, at *1 (N.D. Ill. June, 11, 2010). Spamhaus' ROKSO Frequently Asked Questions page indicates that:

> The Register of Known Spam Operations (ROKSO) is a register of spam senders and spam services that have been thrown off Internet Service Providers 3 times or more in connection with spamming or providing spam services, and are therefore repeat offenders. Spamhaus believes that these known determined professional spam operations are responsible for approximately 80% of spam on the internet.
>
> The ROKSO database collates information and evidence on each spam operation to assist ISP Abuse Desks and Law Enforcement Agencies.
>
> The existence of these known professional spammers, the aliases they use to obtain ISP accounts, their methods and history is vital need-to-know information for the protection of internet networks.

ROKSO FAQ, *supra* note 3.

[226] *See* e360 Insight v. Spamhaus Project, 500 F.3d. 594, 596 (7th Cir. 2007).

[227] *See id.*

[228] *See id.* at 595-96.

district court entered a default judgment against Spamhaus for $11,715,000 in damages and $1,971.05 in litigation costs.[229]

[66] As part of its proposed remedies under the default judgment, e360 requested that the court order ICANN[230] to suspend the Spamhaus.org domain name, which prompted Spamhaus to obtain new counsel and give notice that it intended to appeal to the Seventh Circuit.[231] On appeal, the Seventh Circuit upheld the default judgment, but denied the excessive damages and injunctive relief, and remanded the case for further proceedings regarding damages.[232] In June 2010, Judge Kocoros issued his final decision, reducing the original multimillion-dollar default judgment to a mere $27,002.[233]

---

[229] *See id*. at 597.

[230] *See* INTERNET CORP. FOR ASSIGNED NAMES & NUMBERS, http://www.icann.org (last visited Jan. 17, 2011) (providing information about the organization that manages the allocation of .com, .org, .net, and other top-level domain names). Ultimately, Judge Kocoras of the district court denied the suspension of the domain name. *See* Order, 360 Insight, LLC v. Spamhaus Project, No. 06 C 3958 (N.D. Ill. Oct. 19, 2006), *available at* http://www.icann.org/legal/spamhaus/denial-proposed_order-19oct06.pdf.

[231] *See* Order, 360 Insight, LLC v. Spamhaus Project, No. 06 C 3958 (N.D. Ill. Oct. 19, 2006), *available at* http://www.icann.org/legal/spamhaus/denial-proposed_order-19oct06.pdf.

[232] *See e360 Insight*, 500 F.3d at 606.

[233] e360 Insight, LLC v. Spamhaus Project, No. 06 C 3958, 2010 WL 2403054, at *8 (N.D. Ill. June, 11, 2010). While its case against Spamhaus was still pending, e360 filed suit against Comcast, a major ISP, based upon Comcast's alleged blocking of e360's marketing e-mail messages. *See* e360Insight, LLC v. Comcast Corp., 546 F. Supp. 2d 605, 606 (N.D. Ill. 2008). In its complaint, e360 alleged that Comcast "regularly blocked emails e360 has attempted to send to Comcast customers who have signed up to receive such emails." Complaint at 5, e360Insight, LLC v. Comcast Corp., 546 F. Supp. 2d 605 (N.D. Ill. 2008) (No. 08 C 340), *available at* http://www.spamsuite.com/node/353 (¶19). Among the claims indentified in e360's Complaint are tortious interference with prospective economic advantage; a violation of the Computer Fraud and Abuse Act; a violation of e360's First Amendment rights, and unfair competition and business practices. *Id.* at 7-14 (¶¶ 25-62). In its responsive filing, Comcast denied the allegations and raised the 47 U.S.C. § 230 and 15 U.S.C. § 7701 et seq. immunities, as well as various other defenses under state anti-spam laws, as an affirmative defense. *See* Comcast's Answer and Affirmative Defenses at 20, e360Insight, LLC v. Comcast Corp.,

[67] While this case raised a number of important issues, most notably jurisdiction, Spamhaus' decision not to appear in the federal case meant that the 47 U.S.C. § 230 defense was never a potential factor.[234] Although e360's claims were similar to those in the *Black Ice* and *OptInRealBig* cases, such as defamation and tortious interference with prospective economic advantage, the jurisdictional dispute and default nature of the judgment makes it difficult to analyze the strength of e360's legal arguments and the likelihood of their success on the merits.[235]

[68] The jurisdictional dispute itself raises an interesting question. Is an out-of-state or offshore entity that knowingly incorporates a company into a spam filter responsible for any damages its action cause in the jurisdiction in which the filtered company is located? Several United States cases – including *Bochan v. La Fontaine*[236] and *U.S. v. Ivanov*[237] – and international courts,[238] have examined this question in the online

546 F. Supp. 2d 605 (N.D. Ill. 2008) (No. 08 C 340), *available at* http://www.spamsuite.com/node/370 (¶¶ 64, 65). E360 also filed, and subsequently withdrew, a number of state and federal suits against several anti-spam advocates who criticized the company online. *See E360 Drops Lawsuit Against Feguson* [sic]*, Gunn, and Chien — Again*, SPAM DIARIES (June 2, 2008), http://thespamdiaries.blogspot.com/2008/06/e360-drops-lawsuit-against-feguson-gunn.html.

[234] *e360 Insight*, 500 F.3d at 600 (holding that the district court did not err in concluding that Spamhaus effectively waived his previously asserted defenses). Spamhaus, by abandoning all defenses to the claims against it, did not allow the court to consider the possible merits of the 47 U.S.C. § 230 defense. *See id.*

[235] *See supra* notes 191-209, 225-34 and accompanying text.

[236] *See* Bochan v. La Fontaine, 68 F. Supp. 2d 692, 697 (E.D. Va. 1999) (finding that long-arm jurisdiction in a defamation case extended over Maryland and New Mexico defendants, in part because damage occurred in Virginia to a Virginia-based plaintiff).

[237] *See* United States v. Ivanov, 175 F. Supp. 2d 367, 372 (D. Conn. 2001) (finding jurisdiction over a Russian-based hacker who broke into Connecticut-based databases because the data theft occurred in Connecticut and the plaintiff received threatening e-mails in Connecticut).

[238] *See Aussie Can Sue Over Online Story*, WIRED (Dec. 10, 2002), http://www.wired.com/news/business/0,1367,56793,00.html (permitting Australian magnate Joseph Gutnick to sue Dow Jones in Australia over a story published in the United States).

context. Given the unusual disposition of *e360 Insight v. Spamhaus Project*, it is unclear whether the case opens the door for others to bring lawsuits against Spamhaus and other international block list and spam filter operators in United States courts, or how 47 U.S.C. § 230 would impact such cases.

IX. SETTING THE STANDARDS: REVISING THE CURRENT SAFE HARBOR TO PROVIDE DUE PROCESS

A. The Need for Redress

[69] Spam places both a time and a financial burden on networks and users with its unceasing torrent, and the incentives of e-mail as a marketing tool continue to encourage new spammers to enter the field.[239] At the same time, senders wrongfully accused and labeled as spammers face significant reputational and financial harm.[240] To what standard of conduct and diligence, then, should block list operators be held?

[70] One could argue that market forces are sufficient to keep block lists under control. Under this theory, if a block list is overzealous and generates too many false positives, users will reject it for another, more accurate product.[241] On a macro level, this theory makes sense where a single, legitimate sender's messages (or even Web site) are blocked, unless a large number of users expect to receive the messages, the impact an incorrect block listing has on the community as a whole will be minimal, thereby making any resulting market forces negligible. On the

---

[239] *See Spam, a Lot*, N.Y. TIMES, Jan. 14, 2011, at A26 (estimating that it costs $80 to send a million spam messages); *see also* Final Report, ICT APPLICATIONS & CYBERSECURITY DIV., ITU Study on the Financial Aspects of Network Security: Malware and Spam 20-22 (July 2008), www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-study-financial-aspects-of-malware-and -spam.pdf.

[240] *See* Stophaus, *Fact: Spamhaus Have* [sic] *Added Innocent IP Blocks to Their Blacklists*, BLOGSPOT (Mar. 23, 2009), http://stophaus.blogspot.com/2009/03/fact-spamhaus-have-added-innocent-ip.html.

[241] *See* Zango, Inc. v. Kaspersky Lab, Inc., 568 F.3d 1169, 1177 (9th Cir. 2009).

flip side of this example, the consequences for the sender can be severe, and absent the ability to utilize the courts, he has little recourse, especially when a block list operator explicitly assumes that anyone claiming an incorrect listing is dishonest.[242]

[71] If courts were more willing (and able) to hold major block list and filter operators accountable for their failure to properly police for false positives, and exercise jurisdiction when the list owner knows or should know that its products are being used in the court's region, block list operators would have to take notice. Unfortunately, the broad application of the safe harbors of 47 U.S.C. § 230 to block list and filter operators, as well as ISPs and message board hosts, has made redress in United States courts difficult, if not impossible, absent an extraordinary showing of malice or negligence that might counter the presumption of good faith.[243]

[72] While the 47 U.S.C. § 230 safe harbor is designed to encourage Internet development and avoid the potential chilling effects of *Stratton Oakmont*,[244] it has effectively enabled block list providers to shut down legitimate e-mailers by mistake or inaction, and then decline to remedy the situation with little fear of legal consequences. On one hand, in light of the number of e-mail recipients whose inboxes feel the effect of the major block lists, this is an unacceptable system.[245] On the other hand, given the utility and necessity of spam block lists to maintain the usability of e-mail,[246] eliminating spam block lists from the protections of 47 U.S.C. §

---

[242] *See ROKSO FAQ*, *supra* note 3.

[243] *See* 47 U.S.C. § 230(c)(2)(A) (2006) (noting that "good faith" is a defense to civil liability).

[244] Stratton Oakmont, Inc. v. Prodigy Servs. Co., No. 31063/94, 1995 N.Y. Misc. LEXIS 229 (N.Y. Sup. Ct. May 24, 1995).

[245] *See Spamhaus SBL*, *supra* note 113.

[246] *See State of Spam, A Monthly Report*, SYMANTEC (Aug. 2009), http://eval.symantec.com/mktginfo/enterprise/other_resources/b-state_of_spam_report_08-2009.en-us.pdf ("While overall spam volumes averaged 89 percent of all email messages in July 2009, spam volumes continue to fluctuate. During July 2009, image spam continued to have an impact reaching 17 percent of all spam during one point in

230, and thereby exposing any block list provider to lawsuits for legitimate as well as illegitimate listings, would likely result in rapid deterioration of e-mail as a viable resource.[247]

[73] Based upon the cases and discussion above, the current jurisprudence with regard to 47 U.S.C. § 230 makes it almost impossible for a mislabeled sender to obtain judicial remedy, even where the block list operator created the improper listing with knowledge that the listed party did not actually send any unsolicited bulk commercial e-mail. At the same time, the lack of a legal standard for block list providers, with regard to either due process or objectivity, means that self-help remedies are often minimal or unavailable for the improperly listed party.[248] What is left, then, is a safe harbor whose provisions may go well beyond preventing the lawsuits and disincentives for Internet development.

B. The DMCA as a Model for a Revised 47 U.S.C. §230

[74] The existence of another safe harbor law may provide some significant guidance for lawmakers seeking to retain the protections of 47 U.S.C. § 230 while fixing the challenges for parties improperly placed on spammer block lists: the takedown notice provisions of the Digital Millennium Copyright Act ("DMCA").[249] While the exact provisions of the DMCA may not lend themselves precisely to the block list context, the overall approach of designation, mandated procedures, mandated action, the right to appeal, and protections against abuse, would significantly improve the legal rights of innocent senders, while retaining the protections spam block list operators, and ISPs, currently enjoy for their good-faith actions to preserve the integrity and usability of e-mail.[250]

July. Health spam decreased by 17 percent, while product and 419 spam both saw increases of eight and three percent respectively month over month.").

[247] *See* 47 U.S.C. § 230(a) (2006) (outlining congressional findings that the efficient use of e-mail should be promoted through proper control mechanisms).

[248] *See id.* § 230(c)(2).

[249] *See* 17 U.S.C. § 512(c) (2006).

[250] *See generally id.* § 512.

[75] While some block lists already have procedures similar to the DMCA's takedown notice provisions, such procedures are not standardized.[251] If a statutory takedown notice requirement is adopted, a block list provider who fails to adhere to the takedown procedures will not be able to claim immunity from lawsuit under 47 U.S.C. § 230 any more than an online service provider that ignores takedown notices is immunized from copyright actions under the DMCA.[252]

[76] The first element of a DMCA-like revision to the 47 U.S.C. § 230 safe harbor would to mandate that the party wishing to take advantage of the liability limitation publish a designated point of contact for those wishing to object to block listing.[253] In this way, whether it is a commercial vendor or a volunteer organization that operates the block list, those who wish to notify an operator of an error have a centralized database of contact information from which to work.[254] From a functional perspective, given that the Federal Trade Commission ("FTC") has primary federal jurisdiction over spam complaints pursuant to the CAN-SPAM Act,[255] and maintains a Web-based resource for spam-related issues,[256] it would be logical for the FTC to host the block list provider database. A revised statute need not mandate that providers identify

---

[251] *See* 17 U.S.C. § 512(c)(2). Not all block list providers are equally open to complaints from listed parties or their legal representatives. *See ROKSO FAQ*, *supra* note 3.

[252] *See* 17 U.S.C. § 512(c)(2).

[253] *See id.* ("The limitations on liability established in this subsection apply to a service provider only if the service provider has designated an agent to receive notifications of claimed infringement.").

[254] The DMCA requires service providers to list and keep current contact information for an agent for service of process on the Copyright Office website. *See* 17 USC § 512(c)(2); *see also* U.S. COPYRIGHT OFFICE, ONLINE SERVICE PROVIDERS, SERVICE PROVIDER DESIGNATION OF AGENT TO RECEIVE NOTIFICATION OF CLAIMS OF INFRINGEMENT, *available at* http://www.copyright.gov/onlinesp/ (last visited Jan. 17, 2011).

[255] 15 U.S.C. § 7706(a) (2006).

[256] FED. TRADE COMM'N, SPAM, RULES & ACTS, *available at* http://www.ftc.gov/bcp/edu/microsites/spam/rules.htm (last visited Jan. 17, 2011).

themselves with the FTC, but it should require that providers do so if they intend to take advantage of the safe harbor.[257]

[77] A centralized provider list would assist consumers and businesses that wish to object to an improper block listing, but it would be insufficient without imposing a reasonable standard for response.[258] Under the DMCA, service providers must, upon receipt of a proper takedown notice,[259] "respond[] expeditiously to remove, or disable access to, the material that is claimed to be infringing or to be the subject of infringing activity."[260] Similarly, a revision to the block list safe harbor should require that protected providers act quickly upon receipt of notice, which should include, at a minimum, the server IP address and other technical information to enable the provider to locate and verify the listing.[261]

[78] Under the DMCA, after the service provider has removed or disabled the alleged infringing content, the party responsible for posting the content is entitled to notification of the removal and may file a counter notice to appeal the content's removal.[262] However, this is not an unlimited right to reverse all takedowns, and in the case of "repeat

---

[257] *See* 17 U.S.C. § 512(c)(2).

[258] *See id.* § 512(c)(3).

[259] *Id.*

[260] *See id.* § 512(c)(1)(C). Interestingly, in *Dudnikov v. Chalk & Vermillion Fine Arts, Inc.*, a case involving the application of the DMCA's takedown notice, the Tenth Circuit noted the possibility that a takedown notice could be used maliciously to shut down a competitor. 514 F.3d 1063, 1073 (10th Cir. 2008). The court further noted that, if used in such manner, a takedown notice could provide grounds for a tortuous interference suit. *See id*. The court found that "crediting the complaint as true as we must at this stage of the litigation, and further giving it the solicitous construction due a *pro se* filing, the facts described above are sufficient to permit an inference that [D]efendants tortiously interfered with [P]laintiffs' business." *Id.* (citation omitted).

[261] *See id.*

[262] 17 U.S.C. § 512(g).

infringers," service providers must adopt and provide notice of policies to ensure such users cannot infringe indefinitely.[263] Likewise, a revised 47 U.S.C. § 230 safe harbor should grant block list operator the option to re-list an IP address if the address sends further spam-like e-mail, or if the operator continues to receive spam notices or block requests from its customers pertaining to that IP address.

[79] Moreover, like the DMCA, a revised spam-statute should grant block list operators the opportunity to create and implement a policy to terminate access by repeat infringers.[264] This policy would permit block list operators to ignore certain listing objections and prevent bulk senders from repeatedly claiming improper listing, which force operators to cycle spammers on and off their lists.[265] But such a right of refusal must not be absolute. The revised statute must require good faith refusal based upon objective criteria as to the reputability of the objecting party, rather than the block list provider's subjective determination.[266] As a further barrier against bulk senders' groundless, repeat counter notices, the revised statute should incorporate a misrepresentations penalty provision similar to that of the DMCA.[267]

---

[263] *Id.* § 512(i)(1)(A) ("The limitations on liability established by this section shall apply to a service provider only if the service provider– (A) has adopted and reasonably implemented, and informs subscribers and account holders of the service provider's system or network of, a policy that provides for the termination in appropriate circumstances of subscribers and account holders of the service provider's system or network who are repeat infringers . . . .").

[264] *See id*.

[265] *See id.*

[266] *See ROKSO FAQ*, *supra* note 3 ("Spamhaus regularly receives letters from spammer's [sic] lawyers attempting to claim that all of a spammers [sic] records are in error and demanding all therefore be removed. [Spamhaus] naturally pay[s] little attention to such requests.").

[267] 17 U.S.C. § 512(f) ("Any person who knowingly materially misrepresents under this section– (1) that material or activity is infringing, or (2) that material or activity was removed or disabled by mistake or misidentification, shall be liable for any damages . . . incurred . . . as the result of the service provider relying upon such misrepresentation . . . .").

[80] The revised statute should also adopt an overall "good faith" prerequisite to the safe harbor immunity in (c)(2)(B) – similar to that in (g)(1) of the DMCA[268] – for providers of access control tools.[269] While it is not clear precisely how courts will apply such a good faith requirement to block list operators, one possible understanding is that operators will be held to utilize an objective definition of spam, rather than the various subjective definitions currently in use.[270] Further, if block list operators want to insulate themselves from liability, they should limit blocking to the actual IP address used to send the alleged spam, rather than expanding their block list to include the e-mail address, or Web site, of the perceived beneficiary of the message (i.e. the party whose products are being advertised).[271] Another method block list operators currently employ to protect against liability, which would be limited or prohibited under this proposed model, is to expand their listings to include other customers of

[268] *See id.* § 512(g)(1).

[269] The good faith exception currently applies only to users and interactive service providers per § 203(c)(2)(A). *See* 47 U.S.C. § 203(c)(2)(A) (2006).

[270] Even vendors that claim objective definitions of spam explicitly exercise their own judgment as to when and how entities should be listed. *See, e.g.*, *SBL Advisory, SBL Policy & Listing Criteria*, SPAMHAUS, http://www.spamhaus.org/sbl/policy.html (last visited Jan. 17, 2011) ("The Spamhaus Block List ("SBL") Advisory 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').") (emphasis added); *Frequently Asked Questions, Comments and Answers*, ANONYMOUS POSTMASTERS EARLY WARNING SYS., http://www.apews.org/?page=faq (last visited Jan. 17, 2011) ("[Network addresses from which no spam has originated] are listed because they have been set up by known spammers and spam support operations, most with a demonstrable repeated history of spamming or spamming services. They are also listed if they host websites advertised in spam, as this too falls under spamming services - these listings normally occur if the owners of that network address range do not remove the offenders.").

[271] *See* Mail Abuse Prevention Sys. LLC, v. Black Ice Software, Inc., No. CV 788630, 2000 WL 34016435 (Cal. Super. Ct. Oct. 13, 2000), at *9 ("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.") (citation omitted).

the same ISP from which the spammer sent its message, to encourage those customers to pressure the ISP to change its policies.[272]

C. Balancing the Equities of the Fight Against Spam

[81] This Article's proposal will undoubtedly raise criticism among block lists operators, users and network administrators who believe the current block list operator safe harbor provides effective spam fighting, just as the overall safe harbor is seen as the most efficient way to enable administrators to manage unwanted content while providing the freest possible forum for legitimate discourse and communication.[273] Critics

---

[272] In October 2009, Spamhaus placed *all* IP addresses belonging to Amazon.com's Amazon Web Services Elastic Compute Cloud ("EC2") on its real-time block list after a single EC2 customer used the service to send an e-mail containing viruses and spam. *See* Brooks, *supra* note 5. Spamhaus ignored complaints from other Amazon EC2 customers, and instead required that Amazon directly work with Spamhaus on the issue. *See id.* Spamhaus' refusal to work with individuals was not solely an objective or technical issue; rather, as Spamhaus CIO Richard Cox stated, "[Spamhaus'] policy for delisting is that the spam has to stop and our editors must be convinced it is unlikely to restart when the listing is removed." *Id.* (quote provided by Richard Cox, CIO, Spamhaus).

[273] As David Ardia acknowledged:

> [W]hen intermediaries remove potentially injurious speech, they often do so without providing an opportunity for the speaker to contest the removal or blocking. It is costly for intermediaries to offer dispute resolution procedures to their users. It is far less costly to simply remove speech at the first sign of trouble or to decline to carry controversial speech in the first place. In fact, any increase in the baseline liability for intermediaries will impact their willingness to facilitate potentially injurious speech. A "profit-maximizing intermediary likely will choose the mechanism that is least costly, rather than the one that preserves the most speech."
>
> Moreover, even if intermediaries were capable of determining what speech is tortious or unlawful, it is unlikely that they would be able to adequately weigh or capture the full social value of the speech they are poised to interdict. Accordingly, "if we impose the full social costs of harm from third-party postings on intermediaries, but they cannot capture the full social benefits of those postings, they will respond by inefficiently restricting the uses that third parties can make of the Internet." We would therefore expect to see excessive

may argue that these suggested revisions would effectively eliminate the safe harbor, and quickly lead block list operators to shut down their lists for fear of lawsuits, but this argument disregards several key points.

[82] First, while block lists provide a strong, and overall positive influence on e-mail, the impact of a mistaken or overly broad block listing on a single sender or company can be devastating, especially when neither the block list operator's processes nor the current law provide adequate financial or procedural recourse.[274] Second, even with the safe harbor as it currently exists, block list operators still receive and respond to allegations of improper listings, whether from legitimately wronged senders or true bulk e-mailers seeking to force their unwanted messages through.[275]

[83] Requiring that block list operators follow additional procedural safeguards and act in good faith to obtain safe harbor immunity, especially if coupled with a formal penalty for a blocked party's false reporting, should not substantially increase the number of complaints, or the time or money needed to respond. Rather, it will give true victims of improper block listing a chance to obtain relief when their legitimate requests for assistance go unanswered. While this revision would not itself address all potential issues,[276] it would at least set a standard for block list conduct that could reduce the likelihood of future lawsuits.

> curtailment of speech, as risk-averse intermediaries filter and block all but the most banal speech. This likely would leave us with something akin to what cable television provides: content from a short list of preapproved providers.

Ardia, *supra* note 18, at 391-92 (citations omitted).

[274] *See* discussion *supra* Parts VI-VII; *see also* Ardia, *supra* note 18, at 412 n.194.

[275] *See* discussion *supra* Part VIII.

[276] For example, the international jurisdictional dispute that was at the heart of *e360 v. Spamhaus*. *See* e360 Insight v. Spamhaus Project, Ltd., 500 F.3d 594 (7th Cir. 2007).

X. CONCLUSION: CLOSING THE GAPS, REQUIRING RESPONSIBILITY

[84] Commercial and volunteer block list operators alike affect numerous commercial relationships and the financial health of companies. They exercise, at the very least, indirect control over access to billions of e-mail accounts whose owners are unaware of which block lists filter their inboxes. Because of the significant practical and commercial impacts associated with the list operators' procedures and choices, block list operators should be held to a professional standard of conduct that includes objectivity, reasonable care, and accountability. The current alternative – relying on block list operators' good faith and internal procedures, while granting them broad statutory immunity – is no longer acceptable. Just as letter carriers are held accountable when their actions affect mail delivery,[277] the law must require that block list, and spam filter, operators make every reasonable effort to ensure their actions do not prevent the delivery of legitimate e-mail, and impose consequences when these requirements are not met.

[277] *See* Jen McCaffery, *Missing Mail Found in Roanoke Residence*, ROANOKE TIMES, Dec. 22, 2004, at A1, *available at* http://www.roanoke.com/news/roanoke/wb/xp-15772 (noting that, in December 2004, thousands of pieces of undelivered mail were found in the Roanoke, VA home of a temporary postal worker, who faced up to five years in, and a fine of up to $250,000 for each piece of stolen mail).