SCRIPT-ed

Volume 3, Issue 4, December 2006

Penetrating the Zombie Collective: Spam as an International Security Issue

Andrea M. Matwyshyn[*]

Abstract

Since the mid 1990's, spam has been legally analyzed primarily as an issue of balancing commercial speech with consumers' privacy. This calculus must now be revised. The possible deleterious consequences of a piece of spam go beyond inconvenient speech and privacy invasion; spam variants such as phishing and "malspam" (spam that exploits security vulnerabilities) now result in large-scale identity theft and remote compromise of user machines. The severity of the spam problem requires analyzing spam foremost as an international security issue, expanding the debate to include the dynamic impact of spam on individual countries' economies and the international system as a whole. Spam creation is becoming a flourishing competitive international industry, generating a new race to the bottom that will continue to escalate. Although the majority of spammers reside in the United States and a majority of spam appears to originate in the U.S., spam production is being increasingly outsourced to other countries by U.S. spammers. Similarly, as U.S. authorities begin to prosecute, spammers are moving offshore to less regulated countries. Therefore, spam presents an international security collective action problem requiring legislative action throughout the international system. A paradigm shift on the national and international level is required to forge an effective international spam regulatory regime. Spam regulation should be contemplated in tandem with the development of data security legislation and closing pre-existing doctrinal gaps in contract, computer crime and jurisdiction law, harmonizing all these bodies of law simultaneously across the international system to form a coherent international data control regime.

DOI: 10.2966/scrip.030406.370

---

[*] Assistant Professor of Law/ Executive Director, International Center for Automated Information Research, University of Florida, Affiliate, Centre for Economics & Policy, University of Cambridge. The wishes to thank Jennifer Hill and Abha Joshi who both contributed research to this article, and Cem Paya, Sharon Gordon, Lilian Edwards, and Jum Carroll for their insightful comments and critiques. Comments are invited at matwyshyn@law.ufl.edu.

1. Introduction

Unsolicited commercial email or "spam" has filled inboxes almost as long as inboxes have been in existence. Like the internet itself, spam has undergone evolution as have the legal challenges it presents. Historically, spam has been primarily conceptualized as a legal issue of annoying or unwanted but likely constitutionally protected commercial speech.[1] However, today's spam is fundamentally different; it is no longer the essentially harmless electronic equivalent of postal mail. Rather, spam has become primarily a vehicle for criminal activity that, in particular, harnesses security-compromised machines on an international basis. Consequently, a reconceptualization of our legal frameworks is necessitated. We must now analyze spam first and foremost as an international security issue.

This article examines the definitional complexity of "spam" and its historical evolution from essentially harmless commercial speech to a serious international security threat. Next, this article undertakes a discussion of current regulatory efforts to stem spam and argues that these efforts are suboptimal in part because they do not contemplate spam as an international security issue. Finally, this article analyzes the escalating international spam crisis as a threat to critical international infrastructures, discussing the economic and social significance of increasing participation of developing countries as both spam generators and recipients. By doing so, this article reframes spam as a collective action problem requiring coordinated international effort. Successful regulation analyzes the spam crisis from a user-centered perspective that places such new regulation in context of comprehensive data security legislation and other legislation.

2. Spam Yesterday, Spam Today, Spam Tomorrow: Historical, Economic and Social Context

The term "spam" is, in many ways, an inherently subjective label. "Spam" has meant different things to different people at different points in time. However, regardless of the definitional subjectivity, by any definition, spam is exacting an economic toll on its recipients and the economies of which they are part. It has evolved from merely a problem of annoying commercial speech to a problem of primarily fraudulent speech exposing recipients to security risks. Four critical problems currently exist in crafting a successful social policy approach to spam: (1) definitional uncertainty with regard to what constitutes "spam" and the need to include criminal conduct as part of the definition; (2) a collective action problem in exacting punishment for spammers; (3) increasing outsourcing of spam labor and the internationalization of the industry; (4) overcoming the failed regulatory efforts to date and their inertia.

---

[1] In the United States, the standard for constitutionally protected commercial speech arises out of the Central Hudson test set forth in *Central Hudson Gas & Electric v Public Service Commission,* 447 U.S. 557 (1980). Central Hudson's four-part test asks (1) whether the speech at issue concerns lawful activity and is not misleading and (2) whether the asserted governmental interest is substantial; and, if so, (3) whether the regulation directly advances the governmental interest asserted and (4) whether it is not more extensive than is necessary to serve that interest.

2.1 Problem 1: Definitional Uncertainty and Hesitation in Acknowledging the Arrival of Malspam

Although today the term "spam" is usually associated with unsolicited email communications, the term has been historically used to refer to several different technological phenomena involving unwanted communications. Spam dates as far back as the late 1970's when an employee of Digital Equipment Corporation sent a mass message over ARPAnet[2] advertising his company's opening of offices in California to computer researchers.[3] In the 1980's, participants in MultiUserDomains (MUDs) saw spam in the form of large amounts of data being sent to databases to crash them and generating text using a program to flood a chat session.[4] In 1993, a USENET moderator wrote a buggy program, and unintentionally sent a message over 200 times to a single USENET group,[5] and in 1994, in one of the best known incidents of early spamming, two Phoenix lawyers posted an advertisement for immigration law services on USENET, reaching thousands of USENET groups.[6] It was also through USENET that the first large-scale email harvesting by spammers began to occur, and spam began to arrive through mass emails.[7] Today, it is estimated that 15 billion pieces of spam email are sent out daily,[8] at least 65% of which is sent with intent to defraud.[9] New variants on old themes of spam are also emerging, as spam through instant messaging applications[10] recreates some of the unwanted communication problems previously seen in MUDs.

However, some new variants of spam present entirely new threats: a merger of spammers and virus writers[11] is generating spam which intentionally capitalizes on a user's weak information security to siphon data or computing resources from a user without the user's knowledge. This "malspam" problem is already at a critical level:

---

[2] ARPAnet was the predecessor of the internet and connected a network of university and government machines. It is estimated the message reached approximately 600 users.

[3] D Streitfield, "Opening Pandora's box", (May 11, 2003) *L.A. Times*.

[4] B Templeton, "Origin of the term 'spam' to mean net abuse" @: <http://www.templetons.com/brad/spamterm.html >

[5] Ibid.

[6] R Everett-Church, "The spam that started it all" (Apr. 13, 1999) *Wired* @ <http://www.wired.com/news/politics/0%2C1283%2C19098%2C00.html>; S. Feist, "The Father of Modern Spam Speaks" (Mar. 26, 2002) *CNET* @ <http://dice-cnet.com.com/2008-1082-868483.html>.

[7] For a discussion of social norms and online communities where user postings that upset the community cause harm, *see* L Lessig, *Code and Other Laws of Cyberspace*, (1999) pp. 78-83.

[8] Ibid at 7.

[9] According to the most recent estimates of the Federal Trade Commission, at least 65% of spam contains fraudulent content or attempts to induce the recipient to enter into a fraudulent transaction. In addition to fraudulent content, requests to be removed from spam recipient lists were not honored at least 63% of the time. Federal Trade Commission, "False Claims in Spam" (April 30, 2003) @ <www.ftc.gov>. Spam fraud losses frequently reach as high as $4,000 per victim. The highest median dollar losses reported the FTC were found among victims of the Nigerian Letter fraud, whose losses were approximately $3,864 each. *See, e.g.,* IFCC "2002 Internet Fraud Report" @ <http://www.ifccfbi.gov/strategy/2002_IFCCReport.pdf >.

[10] Known as spim.

[11] B Sullivan, "The Secret Tricks Spammers Use" (August 13, 2003) *MSNBC*.

it is estimated that as much as 80% of all spam currently results from "zombie drones" [12] or security-compromised computers that have been turned into spam platforms controlled remotely by spam senders.[13] A corollary new variant of spam is phishing. During a phishing attack, an attacker sends unsolicited email that "spoofs"[14] sender information to deceive recipients into believing that the unsolicited email originates from a trusted source, such as a financial services provider.[15] The consumer is then directed to a website to "verify" sensitive personal information such as a social security or credit card number.[16] Phishing fraud losses measured between approximately $500 million and $2.4 billion last year in the U.S. alone.[17]

---

[12] T Spring, "Slaying spam-spewing zombie PCs" (June 20, 2005) *PC World* @ <http://www.pcworld.com/news/article/0,aid,121381,00.asp>. Zombie drones are security compromised machines that can be controlled remotely without the user's knowledge for sending spam or other malicious purposes. *See e.g.,* "Primer: zombie drone" (February 1, 2004) *Washington Post* @ <http://www.washingtonpost.com/wp-dyn/articles/A304-2004Jan31.html>; Testimony of Thomas M. Dailey, Chair and President U.S. Internet Service Providers Association, General Counsel, Verizon Online, Before the Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census (June 16, 2004) @ <http://reform.house.gov/UploadedFiles/Dailey%20Testimony1.pdf>. Purchasing spam time on a zombie drone is also relatively inexpensive, costing as little as 3-10 cents per host machine per week. *See*, *e.g.,* "For rent: hacked zombie PCs for net mischief", *NewspaperAsia* @ <http://newpaper.asia1.com.sg/top/story/0,4136,67698-1093276740,00.html?>. *See also* "A new species: Stefan Savage's talk at NDSS" (February 4, 2005) *Sunbreaks* @ <http://sunbreaks.blogspot.com>.

[13] D Bank, "New virus can turn you into a spammer" (January 29, 2004) *Wall Street Journal* @ <http://www.wsj.com>. Also a black market has developed for zero-day exploit code to be included in or used in connection with spam with the going rate currently set at approximately $4,000-$6,000 per exploit. Zero-day exploit code is code which exploits a security vulnerability for which there is no known patch and of which the vendor is not aware. *See e.g.,* G V Hulme, "Zero-day Attacks Expected to Increase" (March 24, 2003) Information Week @ http://www.informationweek.com/story/IWK20030321S0029; Comments of Simple Nomad, Stanford University, Cybersecurity, Research and Disclosure Conference, (November 22, 2003). Professional spam senders are also known to be, among other things, authoring increasingly personal looking emails which contain viruses for the explicit purpose of harvesting email addresses to compile saleable databases for the purpose of sending spam. *Reuters* "The beagle has landed" (January 23, 2004) *Wired* @ <http://www.wired.com>. *See, also, e.g.,* R Hale "Intrusion Crackdown" @

<http://www.itsecurity.com/papers/telenisus.htm>.

[14] Spoofing is defined as sending a message to make it appear as if it is arriving from someone else. *See*, *e.g.,* Webopedia @ <http://www.webopedia.com/TERM/I/IP_spoofing.html> (last visited November 26, 2005).

[15] One entity whose email is spoofed frequently is Citibank. For statistics on phishing *see*, *e.g.,* Antiphishing Working Group @ <http://www.antiphishing.org> (last visited November 26, 2004). For additional discussion of phishing *see*, *e.g.,* Federal Trade Commission, "Phishing alert" @ <http://www.ftc.gov/bcp/conline/pubs/alerts/phishingalrt.htm>; H A Valetk, "Mastering the Dark Arts of Cyberspace: A Quest for Sound Internet Safety Policies" (2004) *Stan. Tech. L. Rev .2 at* 12.

[16] *See* Anti-phishing Working Group @ <http://www.antiphishing.org> (last visited August 15, 2005).

[17] "Good news: 'phishing' scams net only $500 million" (September 29, 2004) *CNET* @ <http://news.com.com/Good+news+Phishing+scams+net+ionlyi+500+million/2100-1029_3-5388757.html>; *see*, also, *e.g.,* C L Webb, "CEOs plan a phish fry" (June 15, 2004) *Washington Post* @ <http://www.washingtonpost.com/wp-dyn/articles/A42917-2004Jun15.html>; "Gartner Study Finds Significant Increase in Email Phishing Attacks: Cost to U.S. Banks and Credit Card Issuers Estimated at $1.2 Billion in 2003" (2004) *Gartner* @

<http://www4.gartner.com/5_about/press_releases/asset_71087_11.jsp>.

Spam has been primarily conceptualized in the U.S. legal literature as a problem of annoying or inconvenient speech,[18] similar to unsolicited postal mail, faxes, and telephone calls.[19] In the EU, on the other hand, spam has frequently been conceptualized as a privacy question, pitting notions of individual privacy against freedom of trade.[20] Although this conceptualization may have been appropriate at the beginning of spam's history, increasingly the risk of security compromise resulting from new variants of spam is at odds with this characterization.[21] These new variants

---

[18] *See, e.g.*, M A Fisher, "The Right to Spam? Regulating Electronic Junk Mail" (2000) 23 *Columbia J.L. & Arts* 363 (arguing that it is likely that regulation of spam will ultimately take the form of rules regarding the labeling of electronic messages); E Goldman, "Where's the Beef? Dissecting Spam's Purported Harms" (2003) 22 *John Marshall J. of Comp. & Info. L.* 13 (arguing that most purported harms of spam are illusory and are already adequately addressed by existing laws or best left to market solutions); S Grossman, "Keeping Unwanted Donkeys and Elephants Out of Your Inbox" (2004) 19 *Berkeley Tech. L.J.* 1533 (arguing that political spam can and should be regulated as part of a general measure restricting the use of all unsolicited bulk emails); J A Marcus, "Commercial Speech on the Internet: Spam and the First Amendment" (1998) 16 *Cardozo Arts & Ent. L.J.* 245 (arguing that regulating spam comports with the Central Hudson test and is needed because spam is not only annoying commercial speech but it also shifts the advertising cost to the consumer); M Sweet, "Political Email: Protected Speech or Unwelcome Spam?", (2003) *Duke L. & Tech. Rev* 1 (arguing that regulation of commercial spam provides little precedent for regulation of political spam).

[19] *See, e.g.*, C E Fogo, "The Postman Always Rings 4,000 Times" (2000) 18 *John Marshall J. of Comp. & Info. L.* (arguing that amending the junk fax law to cover Internet solicitations, or providing civil and criminal penalties for spamming will be the most effective method of curbing spam and the least vulnerable to First Amendment challenges); C M Rice, "Comment: The TCPA: A Justification for the Prohibition on Spam in 2002?" (2002) 3 *N.C.J.L. & Tech* 375 (arguing that amending the TCPA to incorporate spam is not the most effective method of spam regulation); M B Prince and P A Shea, "After CAN-SPAM, How States Can Stay Relevant in the Fight against Unwanted Messages" (2003) 22 *John Marshall J. of Comp. & Info. L.* 29 (arguing in favor of a child protection registry against spam); R C Balough, "The Do-Not Call Registry Model is Not the Answer to Spam" (2003) 22 *John Marshall J. of Comp. & Info. L.* 79 (arguing that the differences between internet spam and telephone telemarketing make an "opt-out" Do-Not-Spam registry an impractical model).

[20] For discussion of EU approaches to spam see, e.g., L. Edwards, "Dawn of the Death of Distributed Denial of Service: How to Kill Zombies" (2006) *24 Cardozo Arts & Ent. L.J.* 23.

[21] *See, e.g.*, E A Alongi, "Has the U.S. Canned Spam?" (2004) 46 *Ariz. L. Rev.* 263 (arguing that because of the international nature of spam an international approach is most promising and that the efficacy of individual national measures is, as yet, unknown); J B Beckham, "Intel v. Hamidi: Spam as a Trespass to Chattels – Deconstruction of a Private Right of Action in California" (2003) 22 *John Marshall J. of Comp. & Info. L.* 205 (arguing that an exception should be recognized by courts in actions sounding in trespass to chattels involving spam); S Cobos, "A Two-Tiered Registry System to Regulate Spam" (2003) *UCLA J.L. & Tech.* 5 (arguing for a National Registry of Businesses to serve as a single tracking source for businesses/individuals sending out mass commercial email mailings); B Dahl, "A Further Darkside to Unsolicited Commercial Email? An Assessment of Potential Employer Liability for Spam Email" (2003) 22 *John Marshall J. of Comp. & Info. L.* 179 (arguing that the proliferation of unsolicited commercial email in the workplace means extra risk for businesses); S M Graydon, "Much Ado About Spam: Unsolicited Advertising, the Internet and You" (2000) 32 *St. Mary's L.J.* 77 (arguing federal legislation is needed to harmonize state level spam regulation); A E Hawley, "Taking Spam Out of Your Cyberspace Diet: Common Law Applied to Bulk Unsolicited Advertising Via Electronic Mail" (1997) 66 *UMKC L. Rev*. 381 (arguing that spam can be controlled by traditional common law tort principles); C Jones, "Email Solicitation: Will Opening a "Spam-Free" Mailbox Ever Be a Reality?" (2002) 15 *Loy. Consumer L. Rev.* (arguing that it is doubtful that consumers will be able to rely on any help that might be offered by legislation in the near future); E E Marks, "Spammers Clog In-Boxes Everywhere: Will the CAN-SPAM Act of 2003 Halt the Invasion?" (2004) 54 *Case W. Res. L. Rev* 943 (arguing that the eradication of spam will occur only through a comprehensive solution involving both market-based and legislative initiatives); E P Marsh, "Purveyors of Hate on the Internet: Are We Ready for Hate Spam?" (2000) 17 *Ga. St. U. L. Rev*. 379 (arguing that in the absence of governmental regulation of privacy data, criminal law should be able to

of spam, which comprise a burgeoning percentage of spam, have turned it into a high-stakes criminal enterprise; spam is now more about crime than about speech.

The primary comparison from a free speech standpoint, postal mail[22] is no longer apt as an analytical tool for spam. The parallel between postal mail and email ends starkly when the security risk of each is taken into effect. One in every 16 emails has been found to carry a virus.[23] Little risk exists that one in every 16 postal mail items will attempt to criminally harm the recipient. Most importantly, perhaps, unlike postal mail, email demonstrates rates of fraud so high that email is potentially being killed as a communication medium. The pervasiveness of spam has impaired users' sense of control over availability of their own systems to the extent that users started to use the internet less as a consequence of spam.[24] This loss of use arises not only out of

---

reach hate spam if it encourages violence to an intolerable degree); G Miller, "How to Can Spam" (2000) 2 *Vand. J Ent. L. & Prac.* 127 (arguing that advertisers should be required to obtain permission before they send advertisements through an internet service provider's system); A Mossoff, "Spam – Oy, What a Nuisance!" (2004) 19 *Berkeley Tech L.J.* 625 (arguing nuisance doctrine presents a viable option for addressing the spam problem); B M O'Neill, "Wireless Spam This Way Comes: An Analysis of the Spread of Wireless Spam and the Present and Proposed Measures Taken to Stop It" (2003) 22 *John Marshall J. of Comp. & Info. L.* (discussing the comparative impact of wireless spam in Japan and the U.S.); D D Simmons, "No Seconds on Spam: A Legislative Prescription to Harness Unsolicited Commercial Email" (1999) 3 *J. Small & Emerging Bus. L. J.* 389 (arguing that spam legislation should include ten elements (1) being federal in scope and (2) precluding a total ban, legislation serving the interests of ISPs should include: (3) an exemption for parties with pre-existing business relationships; (4) an "Advertisement" labeling requirement at the beginning of a UCE's subject line; (5) a two-pronged opt-out system, including a pre-emptive aspect and a prescribed, direct aspect; (6) real-world names and addresses of both the advertiser and (7) the sender; (8) civil damages and attorney's fees for victims of violations; (9) criminal sanctions for UCE senders known as spoofers who forge the origin information in a message; and (10) oversight of the pre-emptive opt-out list and the spoofing provisions by a federal agency); M Simon, "The CAN-SPAM Act of 2003: Is Congressional Regulation of Unsolicited Commercial Email Constitutional?" (2004) 4 J. High Tech L. 85 (arguing CAN-SPAM will be upheld as constitutional in light of First Amendment challenges); D E Sorkin, "Spam Legislation in the United States" (2003) 22 *John Marshall J. of Comp. & Info. L.* 3 (arguing that legislation has little impacted the spam problem and CAN-SPAM is unlikely to change that); J D Sullivan and M B De Leeuw, "Spam After CAN-SPAM: How Inconsistent Thinking Has Made a Hash Out of Unsolicited Commercial Email Policy" (2004) 20 *Santa Clara Computer & High Tech L.J.* 887 (arguing that the analysis of spam conducted via the CANSPAM Act is inadequate); V Toliopoulos, "Regulating Your Internet Diet: the CAN SPAM Act of 1999" (1999) 10 *DePaul-LCA J. Art & Ent. L.* (arguing federal legislation is needed to stem spamming); R Warner, "Spam and Beyond: Freedom, Efficiency, and the Regulation of Email Advertising" (2003) 22 *John Marshall J. of Comp. & Info. L.* (arguing that spam violates freedom).

[22] Email has proven itself to be a fundamentally different medium in its developmental trajectory than postal mail. In 2001, only 8% of U.S. email traffic was spam. However, by comparison, in 2003 40% of traffic was spam and by 2004, this figure rose to 73% of traffic. By comparison, approximately only 40% of U.S. postal service mail is commercial in nature. 25% of internet users have already diminished their use of email because of spam. A parallel cut has not been noted for postal mail due to the presence of commercial communications.

[23] M Binder, "Canada and the E-Economy" @

<http://strategis.ic.gc.ca/epic/internet/inspp-pps.nsf/vwapj/isacc220305-e.pdf/$FILE/isacc220305-e.pdf>.

[24] D Fallows, "Spam: How it is Hurting Email and Degrading the Quality of Life on the Internet" 12 Pew Internet and American Life Foundation @ <www.pewinternet.org>. To date, the FTC has prosecuted under 100 individuals and entities for spam fraud. *See*, *e.g.,* Prepared Statement of the Federal Trade Commission on Unsolicited Commercial Email Before the Committee on Energy and Commerce, Subcommittee on Commerce, Trade and Consumer Protection, Subcommittee on Telecommunications and the Internet, U.S. House of Representatives (July 9, 2003) @ <www.ftc.gov>

annoyance at filtering through their inboxes to find a handful of legitimate messages, but also from fear of fraud.[25]

To date, this fundamental shift in the character of spam toward criminality has not been adequately acknowledged in either the security community or the legal community, neither of which views spam primarily as an issue of security that potentially threatens national critical infrastructures.

2.2. Problem 2: Positive Economic Incentives to Spam with Few Negative Consequences, Especially for Malspam and Phishing

Information thievery ventures are highly lucrative for spammers, with some professional spammer employees earning salaries in excess of $100,000 per year, and spam entity owners earning millions of dollars per year.[26] Consequently, strong financial incentives exist for spammers' innovating technologically to stay in business. Meanwhile, pursuing spammers presents a type of collective action problem; it is in everyone's collective interest to eliminate spammers, however it is in no one's individual interest to allocate adequate resources to eliminate all spammers themselves. For example, for internet service providers, they do not wish to have customers plagued by spam but, until a critical amount of its resources are usurped, an ISP has little incentive to make sure it is now being used as a spammer base or relay point. This collective action problem impacts both the likelihood that entities will self-police and privately pursue spammers through legal action. A similar collective action problem exists on the international level; although the United States ostensibly has most incentive to allocate resources toward attacking the spam problem as both the top spammer and top recipient of spam, this dynamic has begun to shift with the internationalization of spam.

According to some sources, 80% of spam comes from approximately 200 spammers, most of whom reside in the U.S.[27] However, the U.S. FTC has prosecuted under 100 individuals and entities for spam fraud.[28] This limited number of

---

(last visited January 28, 2004). Most of these enforcement actions involved false content and were brought under Section 5 of the Fair Trade Act, alleging that the defendants in question engaged in unfair trade practices. *See e.g., FTC v. G. M. Funding*, No. SACV 02-1026 DOC (C.D. Cal. filed Nov. 2002); *FTC v. Brian Westby*, No. 032-3030 (N.D. Ill. filed Apr. 15, 2003); *FTC v. NetSource One,* No. 022-3077 (W.D. Ky. filed Nov. 2, 2002); *FTC v. Cyber Data*, No. CV 02-2120 LKK (E.D. Cal. filed Oct. 2002); *FTC v. Internet Specialists*, No. 302 CV 01722 RNC (D.Conn. filed Oct. 2002); *FTC v. Patrick Cella et al.*, No. CV-03-3202 (C.D. Cal.) (complaint filed May 7, 2003); *FTC v. K4 Global Publishing, Inc. et al.*, No. 5:03-CV0140-3 (M.D. Ga.) (complaint filed May 7, 2003); *FTC v. Clickformail.com, Inc.*, No. 03-C-3033 (N.D. Ill.) (complaint filed May 7, 2003).

[25] Above, note 9.

[26] Comments of Simple Nomad, Stanford University, Cybersecurity, Research and Disclosure Conference (November 22, 2003).

[27] *See* Spamhaus @ <http://www.spamhaus.org/rokso/index.lasso> (last visited August 16, 2006).

[28] Prepared Statement of the Federal Trade Commission on Unsolicited Commercial Email before the Committee on Energy and Commerce, Subcommittee on Commerce, Trade and Consumer Protection, Subcommittee on Telecommunications and the Internet, U.S. House of Representatives (July 9, 2003) @ <http://www.ftc.gov> last visited January 28, 2004. Most of these enforcement actions involved false content and were brought under Section 5 of the Fair Trade Act, alleging that the defendants in question engaged in unfair trade practices. *See e.g., FTC v. G. M. Funding*, No. SACV 02-1026 DOC (C.D. Cal. filed Nov. 2002); *FTC v. Brian Westby*, No. 032-3030 (N.D. Ill. filed Apr. 15, 2003); *FTC v. NetSource One,* No. 022-3077 (W.D. Ky. filed Nov. 2, 2002); FTC v. Cyber Data, No. CV 02-2120

prosecutions stems from limited agency resources and the ample resources and technology skills of spammers. Spammers' emails frequently pass through numerous relays and switches to obscure the path of the email, making forensics cumbersome.[29] In at least one case, the Federal Trade Commission traced twenty-one separate switches to locate a spammer,[30] and in another the spammer used as many as 514 different email addresses in 35 countries on six continents.[31] Spammers are aware of these constraints on time, money and physical resources to track them.

2.3 Problem 3: The Internationalization of the Spam Industry

Spam is increasingly international in scope, both among recipients and spammers. On the recipient side, four in five messages (80%) sent to U.S. email addresses are spam. Although this percentage represents the highest in the world, the percentage of spam is on the rise throughout the rest of the world as well - in the United Kingdom, spam represents, 52 percent of all email, in Germany, 41 percent, and in Austria, 32 percent.[32] Recipients of spam are no longer primarily U.S. residents.

Similarly, on the production end, although approximately 65% of the world's most prolific spammers reside in the United States,[33] the problem is progressively more international in nature. The United States' hegemony in as top spammer haven is in decline: only approximately only 23% of spam appears to now originate from the U.S.[34] This number is down from 42.53% in 2004.[35] Although the top spammer resides in the U.S., numbers two and three reside in Eastern Europe[36] other countries

---

LKK (E.D. Cal. filed Oct. 2002); *FTC v. Internet Specialists,* No. 302 CV 01722 RNC (D.Conn. filed Oct. 2002); *FTC v. Patrick Cella et al.,* No. CV-03-3202 (C.D. Cal.) (complaint filed May 7, 2003); *FTC v. K4 Global Publishing, Inc*. et al., No. 5:03-CV0140-3 (M.D. Ga.) (complaint filed May 7, 2003); *FTC v. Clickformail.com, Inc.*, No. 03-C-3033 (N.D. Ill.) (complaint filed May 7, 2003).

[29] K Demarrais "Spam Still Gets Around; New Law Hasn't Stopped Junk Email" 1/11/04 *Rec. N. N. J.* B01, 2004 WL59043912.

[30] Ibid.

[31] *FTC v. D Squared Solutions, LLC.* Civil Action No.: AMD 03 CV3108 (N.D. Md. 2003) (complaint asking for injunctive relief to prevent defendants from engaging in unfair business practices in violation of 15 §U.S.C. 53(b) as well as restitution and damages). These addresses included those of the Kuwait Ministries of Communication and Finance, several Korean schools, and the Virginia Community College system.

[32] *See* Spamhaus @ <http://www.spamhaus.org/rokso/index.lasso> (last visited August 16, 2006). *See, also,* B Sullivan "Now, two-thirds of all email is spam" (May 22, 2004) *MSNBC* @ <http://www.msnbc.msn.com/id/5032714/>.

[33] E Millard "War on Spam Reaches Global Proportions" (Jan. 5, 2004) *E-Commerce Times* @ <http://www.ecommercetimes.com>; *see, generally,* J Magee "The Law Regulating Unsolicited Commercial Email: An International Perspective" (2003) 19 *Santa Clara Computer & High Tec. L. J.* 333, 345 (stating that most spam received in Europe is sent by U.S. based spammers and intended for American audiences); *see also* "SpamCon Foundation Creates Legal Fund" (May 7, 2003) *Wa. Post Bus. Wire* @ <http://home.businesswire.com> (last visited August 16, 2005).

[34] "Sophos reveals latest "Dirty Dozen" spam producing countries" (July 24, 2006) @

<http://www.sophos.com/pressoffice/news/articles/2006/07/dirtydozjul06.html> (last visited August 16, 2006).

[35] S Gaudin, "U.S. by far top spam-producing country" (August 25, 2004) @ <http://itmanagement.earthweb.com/secu/article.php/3399591> (last visited August 16, 2005).

[36] Spamhaus, above, note 32.

are entering the spamming marketplace and their market share is increasing. South Korea now generates approximately 7.5 percent of spam, China (including Hong Kong) produces approximately 20 percent, France sends out approximately 5.2 percent, and Spain, approximately 4.8 percent.[37]

The changing character of spam toward primarily a criminal enterprise also drives spam internationalization in production. As spam and malware converge, the spam industry is and will continue to shift toward a closer virtual and physical proximity to malware authors. Most malware code writers now live outside the U.S.[38] Similarly, zombie drones around the world are harnessed by spammers as a method of concealing the origination point of spam, particularly through techniques such as "invisible bulletproof hosting,"[39] a method of track erasing that creates a supposedly untraceable site by using space on legitimate servers. Because ISPs usually shut down a websites and IP addresses used by known spammers, this method of hosting creates an address that changes constantly by shifting among security-compromised systems.

Further, the market in security compromised machines, which now feeds the spam industry, is not a dominantly U.S. market. Recent arrests in Germany and elsewhere have provided useful information into the international market in zombie drones.[40] This market in compromised machines is big international business: the price of these BotNets (DoSNets) was roughly $500 for 10,000 hosts during summer 2004 when the MyDoom and Blaster (the RPC exploit worm) first appeared on the scene. Non-exclusive access to compromised PCs sells for about five to ten cents each per minute currently.[41] An unprotected personal computer can be owned by an attacker in four minutes, and turned into a zombie drone in only 10 hours from anywhere in the world. [42] Approximately 250,000 new zombies are identified per day with approximately 5 million total zombies currently in operation.[43] The greatest incidence of zombies is not in the United States, it is in the EU (26.16 per cent). The United States is second in incidence (19.08 per cent) and China is third (14.56 per cent).[44]

The threat to international critical infrastructure posed by this international market in zombie drones used for spam is severe. For example, one Polish spam group uses over 450,000 compromised systems, "most of them home computers running

---

[37] Sophos, above, note 34.

@ <http://www.sophos.com/pressoffice/news/articles/2006/07/dirtydozjul06.html> (last visited August 16, 2006).

[38] C Thompson, "The E-Infectors" (Feb. 8, 2004) *N.Y. Times Mag.*

[39] B McWilliams, "Cloaking Device Made for Spammers" (Oct. 9, 2003) *Wired.com* @ <http://www.wired.com/news/business/o,1367,60747,00.html>.

[40] J Leyden, "Phatbot arrest throws open trade in zombie PCs" (May 12, 2004) *Register* @ <http://www.theregister.co.uk/2004/05/12/phatbot_zombie_trade/>.

[41] "Clean system to zombie bot in 4 minutes" *Slashdot* @

<http://slashdot.org/article.pl?sid=04/11/30/1932245>.

[42] Ibid.

[43] *See e.g.,* Ciphertrust, Zombie Statistics @

<http://www.ciphertrust.com/resources/statistics/zombie.php> (last visited August 16, 2006).

[44] Ibid. *See, also,* "Rise of zombie PCs 'threatens UK" (March 22, 2005) *BBC* @ <http://news.bbc.co.uk/1/hi/technology/4369891.stm> (last visited August 16, 2005).

Windows high-speed connections" all over the world.[45] Eastern European organized crime syndicates have also begun launching extortion rackets against businesses in other countries, threatening them with attacks from zombie drones compromised through spam.[46] Similarly, according to FBI sources, the Eastern European mafia views spam as its "9 to 5 job."[47]

2.4 Problem 4: Failed Regulatory Efforts and Incorrect Paradigms

When recharacterized as an international security issue that threatens critical infrastructures, the urgency of controlling spam becomes evident. Regulatory efforts have been underway for some time to little avail. With regard to the technology industry, what might be termed "West Coast Code," borrowing Lessig's terminology,[48] anti-spam and anti-phishing working groups have been put in place, generating few results. Similarly, legal regulation or "East Coast Code" appears to have not fared much better.

2.4.1. West Coast Code Regulation: Industry Regulatory Effort Failures and the IETF

Technological measures to address the spam problem have been to date largely ineffectual. The primary source of regulation through this "West Coast Code" has been through the International Engineering Task Force, a cooperative technology body with little transparency into its processes.[49] Two primary proposals were proffered to IETF for authenticating senders and limiting domain name spoofing and repudiation of spam[50] – Sender ID and DomainKeys. SenderID was a proposal offered by Microsoft to authenticate the identities of senders of email and, thereby ostensibly, mitigate the spam problem.[51] Based on the sender's server IP address, SenderID was intended to eliminate domain name spoofing by preventing repudiation of email and holding ISP's accountable for spam sent from through their services by confirming that each email message originated from the internet domain it claimed. Consequently, recipients could seamlessly reject messages that claimed to be from an

---

[45] Ibid.

[46] J Menn, "Deleting Online Extortion" *LA Times* @ <http://www.prolexic.com/news/20041025-latimes.php>. This trend is concerning particularly because numerous U.S. federal agencies, including the Department of Homeland Security, have repeatedly failed cybersecurity review of the Government Accounting Office. D McCullagh, "Homeland Security flunks cybersecurity prep test" (May 26, 2005) *CNET News.com* @ <http://news.zdnet.com/2100-1009_22-5722227.html>.

[47] Comments of Supervisory Special Agent Thomas X. Grasso, Jr., Federal Bureau of Investigation, Fighting Organized Cyber Crime – War Stories and Trends, at DefCon 2006, Las Vegas, August 3, 2006.

[48] Lessig, above, note 7.

[49] C D Marsan, "IETF to lead anti-spam crusade" (April 12, 2004) *Network World* @ <http://www.networkworld.com/news/2004/0412marid.html>; Internet Engineering Task Force, @ <http://www.ietf.org/ (last visited August 16, 2005)>; J. Leyden "IETF aims to can spam" (March 3, 2003) *Register* @<http://www.theregister.co.uk/2003/03/03/ietf_aims_to_can_spam/>.

[50] *See* Microsoft Corporation, SenderID Home Page @

<http://www.microsoft.com/mscorp/safety/technologies/senderid/default.mspx> (last visited August 16, 2005).

[51] Ibid.

IP address that had not been declared by the alleged sender.[52] Several critiques of SenderID were raised, including the fundamental incompatibility of its license terms with those of open source products[53] and a question regarding Microsoft patents of key SenderID technology,[54] leading AOL, for example, to lose faith in the project.[55] Currently the proposal appears to be fatally stalled in the IETF.

DomainKeys, the proposal of Yahoo![56] and Sendmail, was termed a "cryptographic authentication solution"[57] to the problem of phishing; it uses public-key cryptography to let users verify that a message actually comes from the domain that is listed in the sending address. Each ISP or mail provider that implements the system has a private key that it uses to sign all outgoing messages and publishes its public key in the Domain Name System records. In this manner, DomainKeys would also certify that the contents of the message have not been altered in transit. Because all outgoing email servers would "sign" messages using a digital certificate, recipients could reject messages that did not comport with a listing in the World Wide Web registry.[58] Although DomainKeys received more positive responses in the IETF and public debate than SenderID, the technology itself is now in question. It appears that spammers have already begun using the DomainKeys technology to make their messages appear more legitimate.[59] If this is in fact the case, the technology is already of diminished value. Similarly, security researchers have been able to alter the signatures generated through DomainKeys, thereby "breaking" or at least diminishing its efficacy.[60] This research gives credence to the likelihood that DomainKeys cannot long withstand spammer circumventions, if at all.

IEFT, despite its activity on spam in 2004, has been largely silent on the issue of spam since then. Arguably, it admits this failure on an affiliated website;[61] the Anti-Spam Research Group of the Internet Research Task Force of the IETF states that it

---

[52] *See* B Livingston, "Sender ID Declines, Domain Keys Shines" (September 28, 2004) *IT Management* @ <http://itmanagement.earthweb.com/columns/executive_tech/article.php/3413611>.

[53] *See* Apache Foundation @ <http://www.apache.org/foundation/docs/sender-id-position.html> (last visited August 16, 2005); R Lemos, "Sender ID loses supporters" (September 03, 2004) *CNET News.com* @ <http://news.zdnet.co.uk/internet/security/0,39020375,39165420,00.htm>.

[54] *See* Greplaw "Microsoft's Sender ID Patent Apps Released" (September 27, 2004) @ <http://grep.law.harvard.edu/article.pl?sid=04/09/27/0210209&mode=thread>.

[55] *See* J Wagner, "AOL Dumps Sender ID" (2004) *Internet News* @ <http://www.internetnews.com/xSP/article.php/3408601>; J Barr, "Email Sender ID: The hype and the reality" (August 26, 2004) *News Forge* @

<http://www.newsforge.com/article.pl?sid=04/08/26/1326244>.

[56] *See* Yahoo! DomainKeys Homepage @ <http://antispam.yahoo.com/domainkeys> (last visited August 16, 2005).

[57] *See* Yahoo! Media Relations @ <http://docs.yahoo.com/docs/pr/release1143.html> (last visited August 16, 2005).

[58] Ibid.

[59] *See* D Fisher, "Scammers Exploit DomainKeys Anti-phishing Weapon" (November 29, 2004) *EWeek* @ <http://www.eweek.com/article2/0,1759,1732576,00.asp>.

[60] C Linfoot, "Why DomainKeys is Broken" Circleid @

<http://www.circleid.com/article/791_0_1_0_C/> (last visited August 16, 2005).

[61] Anti-Spam Research Group @ <http://asrg.sp.am/> (last visited August 16, 2005).

has not endorsed any particular technologies and does not anticipate doing so in the future.[62] In fact, the group's efforts have been quelled to the point that spammers have managed to paralyze the Anti-Spam Research Group Wiki, which has been "temporarily disabled" until they "set up some authentication to keep the spammers out,"[63] as well as the discussion list archive of the group which consists entirely of spam postings.[64] Even in the instances where these regulatory efforts through computer code have been effective against spam from the standpoint of preventing annoying or unwanted speech and preserving privacy, the extent of criminality implicated by spam today complicates the West Coast Code regulatory picture.

2.4.2. East Coast Code Regulation: Legal Regulatory Approaches

Nascent international spam regulatory efforts are underway but have not yet fully taken shape. The Organization of Economic Cooperation and Development has set up a task force to examine spam and begin making recommendations for international cooperation on spam regulation.[65] Similarly, a London Action Plan was entered into in 2004 by 19 bodies from 15 countries attending the London international spam enforcement workshop organised by the OFT and the US Federal Trade Commission.[66] The Asia Pacific Economic Cooperation ministerial meeting agreed to principles for fighting spam,[67] and the International Telecommunications Union through the World Summit on Information Society has also begun to consider methods of controlling spam.[68] Over 20 countries currently have some variant of spam legislation.[69] Enforcement of these statutes has been spotty, at best, and any deterrent effects of such prosecutions appear to have been minimal.

Meanwhile, in the United States in late 2003, Congress passed legislation to create national uniformity in spam email legal regulation, the Controlling the Assault of Non-Solicited Pornography and Marketing Act (the "CAN-SPAM Act"),[70] which became effective as of January 1, 2004.[71] In general, the CAN-SPAM Act prohibits

---

[62] Ibid.

[63] Ibid.

[64] Ibid.

[65] *See* Organization of Economic Cooperation and Development @ <http://www.oecd.org/department/0,2688,en_2649_22555297_1_1_1_1_1,00.html> (last visited August 16, 2005).

[66] *See* Federal Trade Commission @ <http://www.ftc.gov/os/2004/10/041012londonactionplan.pdf> (last visited August 16, 2005).

[67] *See* Asian Pacific Economic Cooperation @

<http://www.apec.org/apec/ministerial_statements/sectoral_ministerial/telecommunications/2005/annex_e.html> (last visited August 16, 2005).

[68] *See* International Telecommunications Union @

<http://www.itu.int/osg/spu/cybersecurity/presentations/session3_bueti.pdf> (last visited August 16, 2005).

[69] *See* Spamlinks @ <http://spamlinks.net/legal.htm> (last visited August 16, 2005).

[70] 15 U.S.C.A. Sect.7701 et seq. (2003).

[71] Four major technological methods have been used to attempt to regulate spam: accept or white lists, deny lists, filtering, and adding email "postage" to each message. White lists entail maintaining a list of permitted senders and excluding messages not from these permitted senders. *See e.g.,* J Bone, "AT&T Aborts Plans to Block Email" (October 22, 2003) *MSNBC* @

fraudulent or deceptive sender, subject or content information, dictionary attacks[72] and address harvesting.[73] It also requires that the option to opt-out from future mailings be provided in spam email, that such requests are honored, and that sexually explicit materials are clearly labeled as such.[74] Despite the Act's creation of a private right of action for internet service providers (ISPs),[75] the Act pre-empts most state spam statutes, in whole or at least in substantial part.[76] As such, it removes private

---

<http://www.msnbc.msn.com/id/3341685/>. The second method, deny lists, uses rules to refuse acceptance of communication from certain forbidden parties considered to be "bad actors." *See e.g.,* J Waever, "How to End Spam in the Future" (July 9, 2003) *MSNBC* @ <http://www.msnbc.msn.com/id/3078599/>. A third method uses filters based on neural networks or Bayesian networks which are taught to distinguish spam from nonspam. Ibid. The final method involves imposing costs on senders of spam through "postage." Postage comes in various forms – micropayments, "hashcash," which extracts computational costs from senders through solving puzzles that burn CPU cycles, and challenge-response models, which require human attention time. Multiple methods can also be used in tandem. Currently, no reliable system of micropayments exists. *See*, *e.g.,* W Treese, "Putting It Together: Where are the Micropayments" (2003) 7 *NetWorker* 3, 15-17 @ <http://delivery.acm.org/10.1145/950000/940840/p15-treese.html?key1=940840&key2=4583595701&coll=GUIDE&dl=ACM&CFID=16535447&CFTOKEN=93848377>. For a discussion of hashcash, *see e.g.,* A Back, "Hashcash: A Denial of Service Countermeasure" (August 1, 2002) @ <http://www.hashcash.org/hashcash.pdf>. In the context of spam emails, the favored technological method of the moment is imposing a challenge-response model on an unverified sender, such as a Human Interactive Proofs. *See e.g.,* Carnegie Mellon, HIPs @ <http://www.aladdin.cs.cmu.edu/hips/> (last visited May 3, 2006). *See* E Hansen, "Hotmail Tools Fight War Against Spam" (May 8, 2003) *ZDNet* @

http://news.zdnet.co.uk/business/legal/0,39020651,2134436,00.htm .

[72] Dictionary attacks are a type of attack where all possible combinations of passwords or randomly generated email addresses are used to attempt to gain access to a protected resource or an existing email accounts. *See, e.g.,* Weboepedia @

<http://www.webopedia.com/TERM/D/dictionary_attack.html> (last visited May 4, 2006).

[73] 15 U.S.C.A. Sect.7705 (2003).

[74] Ibid.

[75] 15 U.S.C.A. Sect.7707(g) (2003).

[76] States have begun to also regulate in this space, however state statutes which regulate the same type of conduct as the CANSPAM Act were superseded by it. As of December 2003, 31 states had laws regulating the transmission of spam email. None of these statutes contained an outright ban on spam email, but (1) restricted either the categories of recipients of spam email to those with a pre-existing relationship with the sender or to those who otherwise affirmatively consented to spam email or (2) required clear labeling through a subject line containing the letters ADV: or an opt-out method in the text of the spam to prevent future spam email from being sent to the recipient. With a few exceptions, these statutes were largely unenforced by state attorney generals and few suits were brought under them by recipients until recently. *See e.g.,* P Roberts, "Earthlink Wins $16 million in Spam Case" (May 7, 2003) *PC World* @ <http://www.pcworld.com/news/article/0,aid,110627,00.asp>. Cases making use of state level anti-spam email statutes as basis for suit have been relatively sparse, with no more than a few per state. *See, e.g., Microsoft Corporation v. Does 1 through 50*, Case No. 5:03-cv-00644 (N.D. Ca. 2/14/03); *Hypertouch v. Link It Software*, Case No. CIV426832 (San Mateo Supr. Ct. 10/31/02); *Morrison & Forrister v. Etracks.com*, et al., Case No. CIV404294 (San Francisco Supr. Ct. 6/26/02); *Earthlink Inc. v. Doe No.1*: 01-cv-2097 (N.D. Ga. 2001); *Earthlink, Inc. v. Smith*, No.1: 01-cv-2009 (N.D. Ga. 2001); *MonsterHut Inc. v. PaeTec Communications, Inc*., Case No. 107189-cv-2001 (Sup. Ct. Niagara Co. 2001), aff'd 294 A.D.2d 945 (4th Dept. 2002); *People of the State of New York v. MonsterHut, Inc.*, (N.Y. Sup.Ct.,N.Y.Cty.2/3/03); *Verizon Online Services, Inc. v. Alan Ralsky, Additional Benefits, L.L.C. et al.*, Case No. 01-CV-432 (E.D.Va. 2001); *America Online v. CN Productions, Inc.*, Case No.98-552-A (E.D.Va.1998); *Terry Gilman v. Sprint Communications*, Case No. 020406640 (Utah Dist. Ct., 3d Jud.Distr. 5/22/02); *State of Washington v. Jason Heckel, d/b/a Natural Instincts,* No. 98-2-25480-7 SEA (Wash.Super.Ct.,King Co. 3/10/00). In fact, in *Cyber*

rights of action granted by some state anti-spam statutes which have effectively been used by ISP's, nonISP business, and consumers to obtain recourse against spammers.[77] The Act has received mixed reviews at best to date[78] and leaves many loopholes which may catalyze a boom in certain types of spam.[79] Some reports indicate that most spammers, as high as 95%, are ignoring the law or are only making very superficial modifications in connection with it to appear in compliance.[80] This said, a recent $7million settlement reached by Microsoft Corp. with a renowned spammer demonstrates that some recourse is available under the act for determined litigants.[81]

Overall, it is fair to assess both West Coast and East Coast Code regulatory efforts as largely ineffectual in curbing spam and the harms that accompany it. A new approach is warranted.

3. The Race to Preserve Critical Infrastructures: Leveraging Organizational Code Regulation

The ideal regulatory approach will facilitate emergence of a self-sustaining cooperative spam effort among consumers, business and regulators. Through looking at the dynamic interactions of spammers, users, governments and business, patterns in behaviors become visible. These patterns of strategic interaction themselves create a

---

Promotions, Inc. v. America Online, Inc., 948 F. Supp. 436 (E.D.Pa. 1995) it was the sender of spam who sued AOL alleging that AOL's blocking of spam constituted an infringement of First Amendment rights. The court found in favor of AOL, reasoning that AOL was not an instrumentality of the government or performed a traditional government function. Ibid. Similarly, the California and Washington anti-spam email statutes were tested on dormant commerce clause grounds and upheld. *See Ferguson v. Friendfinder*, 94 Cal. App. 4th 1255 (Cal. 2002); *Washington v. Heckel*, 143 Wn.2d 824 (2001).

[77] *See e.g.,* P Queary, "Redmond Man Wins Big in Spam Case" (September 11, 2003) *Seattle Times* @ <http://seattletimes.nwsource.com/html/businesstechnology/2001723719_spam11.html>.

[78] *See e.g.,* C Ulbricht, "Spam Law Generates Confusion" (January 26, 2004) *Wired* @ <www.wired.com>.

[79] *See, e.g.,* "CAN-SPAM law has had limited success in its first year" (Jan 20, 2005) *News Target* @ <http://www.newstarget.com/003569.html> (last visited August 16, 2005). The most significant loophole in the Act arises as a consequence of its overly narrow definition of the spam contemplated by the Act; the Act is limited to email only. 15 U.S.C.A. Sect. 7702 (2003). As such, it has already failed to be adequately technologically neutral to successfully limit the next generation of spam - malspam. Though a positive step in at least starting a discourse on the issue of spam and ethical marketing practices, the CAN SPAM Act will ultimately most likely be of limited effectiveness. Among its other provisions, the Can Spam Act empowers the FTC to create a Do Not Spam registry. 15 U.S.C.A. Sect. 7709 (2003). This centralized information database may become an attractive data harvesting source for spammers if not carefully architected, a conclusion that the FTC itself reached. See Federal Trade Commission, National Do Not Email Registry, A Report to Congress (June 2004) @ <http://www.ftc.gov/reports/dneregistry/report.pdf#search=%22ftc%20do%20not%20spam%20registry%22>.

[80] C Ulbicht, "Spam Travels into Gray Area" (Jan. 29, 2004) *Wired* @ http://www.wired.com/news/technology/0,1282,62087,00.html .

[81] E Chabrow, "In The Fight Against Spam, A Few Knockouts" (Aug. 15, 2005) *Information Week* @ <http://www.informationweek.com/story/showArticle.jhtml?articleID=168601273>.

type of regulation on the system, an "organizational code." Finding and acknowledging these patterns offers guidance for crafting future spam policy.

3.1 Adopting a User-Centric Approach to Spam Regulation

One of the most serious threats posed by spam is a breakdown of user trust in the internet. The goal of many technologists and legislators in crafting approaches to both spam and to internet security generally has been to construct a technological and legislative "black box," excluding users from their own protection and governance as much as possible. Although such an approach is undoubtedly more elegant a structure from an engineering standpoint, it falls short on building user trust in the medium. Although some users may be growing numb to yet another email about herbal supplements, others are using the internet less as a consequence of spam.[82] The more virulent strains of spam will undoubtedly further erode their trust in the internet as a commercial medium. Spam is a social problem that will not be remedied by enlisting only a few members of society. In a world where the vast majority of users receive spam generated by the security-compromised machines of other users, the calculus of free speech versus consumer protection begins to shift. Users must be helped to learn to protect themselves or at least feel included in their own protection. Specifically, a user-centric legislative and technological approach is one that is constructivist in nature.

Constructivist learning occurs in the space between a user and the technology, helping the user learn to help herself. A constructivist approach is inherently situated and interactive; it recognizes that a user's knowledge is perspectival and evolutionary. A constructivist approach to spam remediation will assist the user in building an internal body of knowledge and experience that is continually open to modification and expansion. One of the goals of this type of learning is the transference of control from the teacher to the student and to encourage students to socially construct meaning with peers on an ongoing basis.[83] In other words, a successful approach to building trust with users is to include them in the security equation and to construct regulation that assists users in becoming progressively more independent learners about technology.[84]

Reviewing the regulatory approaches of most countries, an approach driven by users' experience and learning about spam does not appear to be emerging. Users perceive their privacy interests, control over their inbox and ability to protect themselves against financial data being stolen online as intrinsically interwoven. Users seek an end-to-end solution. Meanwhile, legislative approaches are usually

---

[82] Fallows, above, note 24.

[83] *See, e.g.*, A K Bednar, D. Cunningham, T M Duffy, and J D Perry, "Theory into practice: How do we link?" *in* T M Duffy and D H Jonassen (*eds*), *Constructivism and the Technology of Instruction: A Conversation*, (1995) p103-104.

[84] One approach for enabling those who receive spam to fight back has been offered by Lawrence Lessig, who has argued that a bill offering bounties for spammers is one useful approach to remedying the amount of spam. *See, e.g.,* D McCullagh, "Perspective: A Modest Proposal to End Spam" (April 28, 2003) *CNet* @ <http://news.com.com/2010-1071-998513.html>. Although this type of approach would undoubtedly be successful to a certain extent, the internationalization of the spam industry would render its effectiveness limited as the bounties would be on a US national basis.

compartmentalized, rarely discussing computer intrusion concerns as part of spam regulation and rarely providing a concrete course of action for a victimized user.

3.2 Stopping the "Spam Red Queen Effect"

An arms race exists between spammers and the technologists who fight them. This dynamic set of interactions in the spam arms race might be termed the "Spam Red Queen Effect."[85] In the context of spam, this Red Queen Effect involves spammers working to write spam dissemination programs which can circumvent current technological anti-spam protections in place,[86] while, simultaneously, the leading minds in industry at entities such as Microsoft and Yahoo! race against them to foil these new spamming products. For instance, when industry resorted to puzzles that required human input to enable transaction processing, it is believed that spammers outsourced the human labor of performing these puzzles called human interactive proofs or HIPs[87] to workers in developing countries.[88] It is part of this evolutionary research and development process of spammers that has also lead to the merger of virus writers and spammers and the ascendancy of malspam and phishing; spammers are innovating to stay one step ahead of technological spam regulation. Information criminals' ability to continue their activities is dependent on their ability to constantly innovate, which they will undoubtedly continue to do successfully.

Although keeping up with spammer innovation is critical, the current arms race is part of what has pushed spammers toward increasing criminality. This continuing escalation will inevitably result in spammer attempts to compromise increasingly more sensitive infrastructures. The idea of a botnet army turning on its owners and their critical infrastructures was a thing of science fiction for most people ten years ago; today, it is entirely plausible. A new type of regulatory approach focused on long term technology and legal solutions is needed more critically than another round of small technology "fixes." Technology alone will never solve the social problem of spam; coordinated long term efforts among technologists, lawyers, regulators and users are needed.

---

[85] *See e.g.*, Wikipedia @ <http://en.wikipedia.org/wiki/Red_Queen> (last visited August 16, 2005). A Red Queen Effect generally refers to a situation where individuals must adjust quickly to changing threats to survive from generation to generation, derived from Lewis Carroll's *Through the Looking Glass*, where Alice complains to the character of the Red Queen that it is necessary to run simply to stay in the same place and advancing means running twice as fast *See* Lewis Carroll, *Through the Looking Glass and What Alice Found There* (1872) @ <http://www.online-literature.com/carroll/lookingglass/> (last visited August 16, 2005).

[86] For example, increasingly spam messages include "chaff" – strings of characters that appear randomly generated for the purpose of confusing spam filters, which presume that only a legitimate message would contain such a string. For a discussion of chaff *see, e.g.,* G Hulten, A Penta, G Seshadrinathan and M Mishra, "Trends in Spam Products and Methods" @ <http://www.ceas.cc/papers-2004/165.pdf> (last visited March 1, 2005).

[87] HIPs are security puzzles used to verify that the sender of an email is a human and that the email is not an automatically generated bulk spam email from a machine. *See e.g.,* Carnegie Mellon "HIPs" @ <http://www.aladdin.cs.cmu.edu/hips/> (last visited January 28, 2004).

[88] *See e.g.,* SpamCop list (August 16, 2001) @ <http://news.spamcop.net/pipermail/spamcop-list/2001-August/018361.html> (last visited March 6, 2005). *See also, e.g.,* N Vidyasagar, "India's secret army of online ad 'clickers'" (May 3, 2004) Times News Network @

<http://timesofindia.indiatimes.com/articleshow/msid-654822,curpg-1.cms>.

3.3 Working toward a Race to the Top and Preventing a Race to the Bottom

Returning to a classical debate in corporate law theory about jurisdictions and regulatory competition, any spam regulation, whether technological or legal, can contribute to jurisdictional competition for spammers and users. Regulators should be sensitive to the dynamics of organizational code their work sets in motion. In other words, every policy initiative should be carefully analyzed to determine whether the resulting strategic interactions of players in the marketplace will occasion a "race to the bottom"[89] or a "race to the top"[90] for spam policy. Current regulatory efforts to date both on the technology end and on the legal end appear to have fallen short in this regard of working toward encouraging a race to the top. In the United States, the CAN-SPAM Act has been largely ignored or only superficially followed. DomainKeys has already been broken prior to large scale implementation.

Perhaps more promising regulatory approaches are those which attack not the spam itself, but the international infrastructures that enable the industry to exist, such as those of financial intermediation and money transfers. Perhaps through refocusing our efforts not solely on the spam itself but on these structures which indirectly buttress it, a coordinated effort will produce greater results. For example, part of the problem stems from spammers getting access to email lists through security breaches. Remedying problems of weak enterprise security will have positive ripple effects into the spam problem, and prosecuting breaches of information security by insiders may lead to spammers purchasing the stolen information.[91] By encouraging a race to the top in other areas of law and international cooperation through the vehicle of spam, a race to the top in the area of spam regulation is similarly more likely.

4. The Legal Answer: A Pro-Active International Legal Approach

Two important legal lessons can be learned from the evolution of the spam problem. First, the spam problem demonstrates that technologists cannot always solve technology policy problems. Some technology-caused problems trigger social problems that extend far outside the realm of bits and bytes. When average consumers become a technology's end users, a boundary is crossed that incentivizes information crime and a Red Queen Effect scenario is likely to develop, putting technologists into an arms race. Second, narrow technology-specific regulatory solutions to these problems will also usually fail at the point a Red Queen Effect begins. At that point, it is too late for a narrow, technology-specific legal solution to be effective; market incentives for information criminals are too strong. Crafting a narrow legislative

---

[89] *See, e.g.,* L Bebchuk, A Cohen and A Ferrell, "Does the Evidence Favor State Competition in Corporate Law?" (2002) 90 *Cal. L. Rev.* 1775.

[90] *See e.g.,* R Romano, "Competition for Corporate Charters and the Lessons of Takeover Statutes" (1993) 61 *Fordham L. Rev.* 843.

[91] For a discussion of enterprise security and its connections to spam, see, e.g, A M Matwyshyn, "Material Vulnerabilities: Data Privacy, Corporate Information Security and Securities Regulation" (2005) 3 *BBLJ* 129. An argument can be made that the EU already demonstrates a more rigorous data control regime than that of the U.S. and that enforcement problems experienced in the EU would be replicated in the US if more stringent data control legislation was implemented. As such, some scholars argue that a levy on data processing profits is needed. See, e.g., L Edwards, "The Problem with Privacy - A Modest Proposal" (2003) 3 *Privacy and Data Protection* 6.

approach merely enables spammers to morph the regulated technology to easily fall outside the legislative parameters.

Existence of a Red Queen Effect signals a technology policy failure and only a cooperative multilateral effort across legal regimes can address the problem. The case of spam, especially malspam, in its current incarnation forces us to address complicated legal questions surrounding information markets generally. The markets in personally identifiable consumer information have expanded in scope dramatically since the mainstreaming of the internet, and law has been slow to respond. Regulating these information markets and the businesses that they foster presents the only long-term solution to the problems raised by spam.

As data breaches and losses of consumer information by governments and corporate entities become more frequent, the connection between these security breaches and the escalation of the spam problem should be recognized. A successful technological and legal regulatory approach will harmonize the impact of technology and law to consider data security, privacy, criminal intrusion, spam regulation and user recourse in one, internally consistent package. The judicial and legislative approaches to criminal computer intrusion law and civil recourse for spam, at least in the United States, have been inconsistent. Recourse for privacy breaches is only now being debated.

Legally defining adequate standards of care for consumer data through uniform legislation and, in common law countries, court decisions developing law of data negligence and due care can begin to chip away at the spam problem. Only a holistic legal approach of this sort can generate market forces to make spam less profitable. Through making customer lists more difficult to obtain, we raise the costs of spamming. By legally mandating reasonable pre-emptive data security precautions, we help businesses and governments help themselves with the spam problem and data vulnerability generally. Costs of spamming can be further increased through allocating legislative attention to the consumer education side of the problem discussed earlier. When carefully crafted comprehensive data security regulation begins to work in tandem with technological measures and a more educated user base, problems of spam and malspam will begin to slow in their development.

However, even this broader legislative approach to problems such as spam will fail until the international legal underpinnings of a successful regime are put in place. On an international level, gaps in legal frameworks not specific to spam pose obstacles to a coherent spam regime. Efforts should be refocused on an international basis on harmonizing three key legal areas – contract law, computer intrusion and information theft law, and law related to international jurisdiction and judgments. Because of the definitional subjectivity of spam, the primary common threat that separates spam from nonspam is whether the user wished to receive the particular email, i.e. user consent, a contract law concept. Even when consumer consent exists, the behavior of the spam in question can exceed the boundary of that consent and harm the consumer in a criminal manner. Criminal computer intrusion law is then triggered and an intent-based legal regime for addressing spam may hold more promise. Finally, because an information criminal can conduct operations from anywhere is the world, international conventions on jurisdiction, judgments and extradition are required to eliminate jurisdictional arbitrage by spammers. For example, the proposed Hague

Convention on Jurisdiction and Foreign Judgments in Civil and Commercial Matters[92] appears stalled, which is a disincentive to entities who might otherwise be inclined to sue spammers in foreign jurisdictions and an incentive to spammer mobility. Similarly, the international Convention on Cybercrime has not been universally ratified, with the United States Congress ratifying the US joining in August 2006.[93] Consequently, any meaningful legislative approach to spam must consciously address these legislative obstacles and contemplate recourse end-to-end for spam abuses. Through focusing on the evolutionary nature of spam and assessing these bodies of law in tandem, technological tools and legal recourse can be more effectively crafted.

Finally, a dose of legal reality in our approaches in required. A goal of eliminating all spam is neither achievable nor is it even necessarily optimal in a world of scarce enforcement resources; instead, the legal goal is better articulated as attempting to dissuade the majority of would-be information thieves from engaging in this behavior. The most determined information criminals will find a way to thwart our best legal and technological efforts, but currently even relatively unskilled thieves succeed. An achievable goal is creating a system that minimizes the percentage of information criminals with the resources and technology skills needed to keep their enterprise profitable. At the point the vast majority of would-be information criminals are deterred, we will have achieved an excellent legal starting point. We are not yet there.

5. Conclusion

Spam has been technologically transformed in the last decade from primarily relatively harmless commercial speech to a critical security issue which poses a threat to the viability of international infrastructures. Consequently, our legal and policy frameworks for analysis of the spam problem must be reassessed accordingly. As greater numbers of security-compromised computers become harnessed by spammers for criminal activity, new and more serious modes of criminality will arise. Crafting a cooperative, international approach to the spam problem that generates cooperation among users, technologists and lawyers presents an urgent undertaking.

---

[92] *See* CPTech @ <http://www.cptech.org/ecom/jurisdiction/hague.html> (last visited August 16, 2005).

[93] *See, e.g.,* U.S. Department of Justice, International Aspects of Cybercrime @ <http://www.usdoj.gov/criminal/cybercrime/intl.html> (last visited August 20, 2006).