Boston College International and Comparative Law Review

Volume 29 | Issue 2 Article 6

5-1-2006

International Spam Regulation & Enforcement: Recommendations Following the World Summit on the Information Society

Meyer Potashman

INTERNATIONAL SPAM REGULATION & ENFORCEMENT: RECOMMENDATIONS FOLLOWING THE WORLD SUMMIT ON THE INFORMATION SOCIETY

MEYER POTASHMAN*

Abstract: Unsolicited bulk e-mail, or "spam," is often called the scourge of the information age. Because of the cross-border nature of the Internet, both governments and the private sector are facing many challenges in combating cross-border spam. In recent years, through the World Summit on the Information Society (WSIS), the international community has committed itself to fight spam on a global level through increased cooperation and enforcement of spam laws. This Note evaluates many of the issues involved in preventing cross-border spam, discusses the latest methods of enforcement in both the private and public sectors, and recommends an approach to the problem in light of the commitments made at WSIS.

INTRODUCTION

Unsolicited bulk e-mail, or "spam," is widely considered to be the scourge of the information age.[1] Millions of unwanted e-mail messages sent every day affect virtually everyone with an e-mail account.[2] These spam messages cost Internet Service Providers (ISPs) and Internet users millions of dollars due to lost productivity and technical resources.[3] To some extent, the rise of spam has slowed the spread of the Internet

* Meyer Potashman is a Production Editor of the *Boston College International & Comparative Law Review.*

[1] U.N. INFO. & COMMC'N TECHS. TASK FORCE, GLOBAL FORUM ON INTERNET GOVERNANCE—INFORMAL SUMMARY 11 (2004), *available at* http://www.unicttaskforce.org/perl/documents.pl?do=download;id=565.

[2] *See, e.g.*, ROBERT HORTON, INT'L TELECOMMS. UNION, ITU WSIS THEMATIC MEETING ON COUNTERING SPAM, CHAIRMAN'S REPORT ¶ 11 (2004), *available at* http://www.itu.int/osg/spu/spam/chairman-report.pdf; *see also* CLAUDIA SARROCCO, ITU WSIS THEMATIC MEETING ON COUNTERING SPAM: SPAM IN THE INFORMATION SOCIETY: BUILDING FRAMEWORKS FOR INTERNATIONAL COOPERATION 4 (2004), *available at* http://www.itu.int/osg/spu/spam/contributions/Background%20Paper_Building%20frameworks%20for%20Intl%20Cooperation.pdf (noting that spam represents up to 76% of all e-mail traffic).

[3] SARROCCO, *supra* note 2, at 4.

and related technologies in the developing world as well.[4] The public and private sectors have proposed many technical and legal approaches to combating spam.[5] One key obstacle in this fight, however, is the political boundaries between independent states.[6] The Internet, of course, has no boundaries, so spam can easily travel from one country to the next, making it difficult to track down its senders.[7] In recent years, several countries have passed laws criminalizing spam, but without international cooperation, it is difficult to enforce these laws against foreign spammers.[8]

The United Nations has convened a two-part summit meeting to address this and other Internet-related issues.[9] Known as the World Summit on the Information Society (WSIS), the summit first convened in Geneva in 2003 and met again in November 2005 in Tunis.[10] At the various summit meetings, the international community committed itself to the fight against spam.[11] This Note will explore the anti-spam options that the international community discussed in these forums, as well as some steps for continuing the fight against spam in the future. Part I provides some background to the spam problem,

---

[4] *See* Contribution to the ITU WSIS Thematic Meeting on Countering Spam From Kenya, Sudan, Tanzania And Zambia (2004), *available at* http://www.itu.int/osg/spu/spam/contributions/Developing%20countries_contribution.pdf [hereinafter Developing Nations Contribution].

[5] *See generally* Horton, *supra* note 2, ¶¶ 16–34.

[6] *See* John Magee, *The Law Regulating Unsolicited Commercial E-Mail: An International Perspective,* 19 Santa Clara Computer & High Tech. L.J. 333, 378 (2003) ("The jurisdictional problems created by the proliferation of transborder unsolicited e-mail communications represent what may prove to be an insurmountable hurdle.").

[7] *See* Sarrocco, *supra* note 2, at 17.

[8] For a summary of international spam laws, see David Sorkin, Spam Laws, http://www.spamlaws.com (last visited Mar. 7, 2006). For a summary of the jurisdictional challenges in enforcing spam, see Philippe Gérard, Int'l Telecomms. Union, ITU WSIS Thematic Meeting on Countering Spam: Multilateral and Bilateral Cooperation to Combat Spam 10–12 (2004), *available at* http://www.itu.int/osg/spu/spam/contributions/Background%20Paper_Multilateral%20Bilateral%20Coop.pdf.

[9] *See* Wendy M. Grossman, *Nations Plan for Net's Future,* Wired News, Oct. 11, 2004, http://www.wired.com/news/technology/0,1282,65254,00.html.

[10] Hans Klein, Understanding WSIS: An Institutional Analysis of the UN World Summit on the Information Society 3 (2003), *available at* http://www.ip3.gatech.edu/images/Klein_WSIS.pdf.

[11] World Summit on the Info. Society, Declaration of Principles (WSIS Doc. No. WSIS-03/GENEVA/DOC/0004) (2003) ¶ 37, *available at* http://www.itu.int/dms_pub/itu-s/md/03/wsis/doc/S03-WSIS-DOC-0004!!PDF-E.pdf [hereinafter Declaration of Principles] (noting the Geneva summit's commitment to address the spam issue); World Summit on the Information Society, Tunis Agenda for the Information Society (WSIS Doc. No. WSIS-05/TUNIS/DOC/6 (Rev. 1)-E) (2005) ¶¶ 41–42, *available at* http://www.itu.int/wsis/docs2/tunis/off/6rev1.html [hereinafter Tunis Agenda].

attempted technical and legal solutions, and the current state of international spam cooperation. Part II discusses the various issues involved in defining spam, global "Internet governance," the crafting of spam laws, and the compromises inherent in international solutions to the problem. Finally, Part III suggests some recommendations on how to put in action the goals of WSIS by structuring a flexible yet effective international anti-spam regime.

I. Background & History

During the relatively short history of the Internet, spam has grown into a major problem, prompting action by many different parties and institutions around the world.[12]

A. *Spam's Harmful Effects*

Though people define spam in several different ways, in general, people consider many kinds of unwanted e-mail to be spam.[13] Spam ranges from unsolicited yet legitimate sales pitches, to pitches for objectionable yet possibly legitimate services such as pornography and other sexually-explicit materials.[14] Spam also encompasses a wide range of advertisements for pharmaceuticals of questionable origin, mortgages, pyramid schemes, and other goods and services, many of which are purely fraudulent.[15] Some of the more damaging types of spam are those that include computer viruses and identity-theft schemes, which attempt to induce recipients to reveal sensitive personal information.[16]

The spam problem has increased dramatically throughout the world in recent years.[17] Spam is estimated to account for around 76% of all e-mail traffic.[18] It is estimated to cost Internet users worldwide around $10 billion per year, which excludes productivity and direct financial losses caused by viruses and identity theft.[19]

---

[12] *See* Am. Civil Liberties Union v. Reno, 929 F. Supp. 824, 830–34 (E.D. Pa. 1996) (providing an overview of the history of the Internet); Gérard, *supra* note 8, at 3–6.

[13] *See* David E. Sorkin, *Technical and Legal Approaches to Unsolicited Electronic Mail*, 35 U.S.F. L. Rev. 325, 327–35 (2001).

[14] *Id.* at 336; Magee, *supra* note 6, at 339.

[15] For an overview of types of spam, see VirusList.com, Types of Spam, http://www.viruslist.com/en/spam/info?chapter=153350533 (last visited Mar. 7, 2006).

[16] *See* Sarrocco, *supra* note 2, at 9–10.

[17] *See* Gérard, *supra* note 8, at 4.

[18] Sarrocco, *supra* note 2, at 4.

[19] *Id.*

The problem with spam is that it is profitable, largely because its costs are shifted from the spammers to their recipients.[20] Unlike direct postal mail, where the sender pays for each message, the cost to the sender of each e-mail is negligible.[21] Thus, spammers can market their wares to millions of people with minimal cost to them.[22] They only need to convert a small fraction of their messages into sales to reap a significant profit.[23] Their recipients and ISPs, however, bear the costs in several ways.[24] Users lose time, and sometimes access fees, "sifting through, identifying, and deleting the messages," as well as in attempting to unsubscribe from spam lists or updating their spam filters.[25] Similarly, ISPs suffer as their servers and network capacity become clogged with spam, forcing them to expand their resources to account for the spam on their networks.[26] An increase in spam on an ISP's network also affects that ISP's goodwill and could result in customer turnover as customers abandon their spam-clogged e-mail accounts for alternative addresses with other providers.[27] These costs ultimately are shifted to consumers in higher access fees.[28] In addition to the financial costs of spam, the plethora of sexually explicit spam raises concerns for parents who do not want their children exposed to such messages.[29]

Spam has also had a particularly harsh effect on developing economies, which are still in the process of building their Internet and communications infrastructure.[30] In sub-Saharan Africa, for example, Internet access is often satellite-based and very expensive.[31] As this expensive bandwidth is clogged with spam, it becomes difficult for ISPs to justify continuing their services.[32] To compound this problem, some

---

[20] Magee, *supra* note 6, at 338; Ho Khee Yoke & Lawrence Tan, Int'l Telecomms. Union, ITU WSIS Thematic Meeting on Countering Spam: Curbing Spam via Technical Measures: An Overview 3 (2004), *available at* http://www.itu.int/osg/spu/spam/contributions/Background%20Paper_Curbing%20Spam%20Via%20Technical%20Measures.pdf.

[21] Magee, *supra* note 6, at 338.

[22] Yoke & Tan, *supra* note 20, at 4.

[23] *See id.*

[24] *See generally* Magee, *supra* note 6, at 338–39 (explaining how costs are shifted away from spammers).

[25] *Id.* at 338.

[26] *See id.* at 339.

[27] *See id.* (noting that spam may cause ISPs to lose business and suffer reputation damage "due to continued clogged bandwidth").

[28] *Id.*

[29] *See id.*

[30] *See* Developing Nations Contribution, *supra* note 4.

[31] *Id.*

[32] *Id.*

users would rather not pay for expensive Internet services at all if the bulk of what they pay for is wasted on spam.[33]

B. *The Most Damaging Types of Spam*

The most damaging spam, which causes considerable harm to the world's economies, consists of those messages that spread viruses, frauds, and scams.[34] These messages turn spam from a mere annoying marketing method into a more damaging tool to invade recipients' privacy and to separate them from their money.[35] Many messages are sent through computer viruses, such as the infamous "Melissa" virus, that automatically resend messages to people on a recipient's contact list.[36] Sometimes viruses turn computers into "zombies," enabling a spammer to take advantage of an innocent user's Internet connection and helping the spammer disguise his or her identity.[37] It is estimated that "zombies" are responsible for a high percentage of all spam sent.[38] Age-old scams, such as the "Nigeria Letter" e-mail, that purport to offer large sums of money to recipients in exchange for sending an initial deposit are also very prevalent forms of spam.[39]

Another common spam threat is known as "phishing."[40] This is an identity theft method through which spammers attempt to obtain user's passwords by sending fraudulent e-mails purporting to be from financial service providers.[41] These e-mails generally misdirect recipients to a false website where users are prompted to reveal sensitive information that the senders can then use to liquidate the recipient's assets.[42]

---

[33] *Id.*

[34] *See* SARROCCO, *supra* note 2, at 9–10.

[35] *See id.* at 9.

[36] *See* Magee, *supra* note 6, at 339–40; YOKE & TAN, *supra* note 20, at 3.

[37] YOKE & TAN, *supra* note 20, at 5.

[38] Grant Gross, *Is CAN-SPAM Working?: One Year After It Went into Effect, Many Say the Nation's Antispam Law Is Ineffective,* PC WORLD.COM, Dec. 28, 2004, http://www.pcworld.com/news/article/0,aid,119058,00.asp (stating that over a three week period in late 2004, a study found that 69% of all spam sent was sent through "zombie" computers).

[39] SARROCCO, *supra* note 2, at 9.

[40] *See id.* at 9–10. *See generally* DAVE BRUNSWICK, TUMBLEWEED COMMC'NS ANTI-PHISHING WORKING GROUP, THE RISE OF PHISHING (2004), *available at* http://www.itu.int/osg/spu/spam/presentations/BRUNSWICK_Session%202.pdf.

[41] SARROCCO, *supra* note 2, at 9–10.

[42] *Id.*

C. *Spam as an International Issue*

The spam problem has many international dimensions.[43] Fundamentally, the Internet does not have any national boundaries.[44] At its core, it is a mechanism for connecting multiple computers and is intended as a loose and virtually ungovernable network.[45] The only component of the Internet that arguably corresponds to states is what is known as the Country Code Top-Level Domain (ccTLD) system.[46] This is the system that assigns the last section of Internet addresses to names corresponding to countries (such as www.bbc.co.uk for the UK, or www.amazon.fr for Amazon's French site).[47]

It is generally impossible to determine a spam's originating country based on its sender's e-mail address.[48] This creates a system in which any national spam laws are difficult to enforce.[49] Even if plaintiffs and prosecutors can locate a spammer or his service provider, they often lack jurisdiction to bring these defendants to court.[50] Further, even if a country would be willing to extend jurisdiction beyond its national boundaries, it can be very difficult to enforce a judgment against such a defendant.[51]

D. *Technical Approaches to Combating Spam*

As the spam problem continues to grow, many organizations have developed anti-spam technologies.[52] The technical problems with dealing with spam are largely related to the minimal security built into e-

---

[43] *See generally id.*

[44] *Id.* at 17.

[45] *See* Vinton G. Cerf, *"First, Do No Harm," in* INTERNET GOVERNANCE: A GRAND COLLABORATION 13, 14 (Don MacLean ed., 2004), *available at* http://www.unicttaskforce.org/perl/documents.pl?do=download;id=778 [hereinafter INTERNET GOVERNANCE] (noting that "the Internet has evolved openly, freely," and without government intrusion).

[46] *See generally* Michael Geist, *Governments and Country-Code Top Level Domains: A Global Survey, in* INTERNET GOVERNANCE, *supra* note 45, at 282 (discussing the role of national governments in managing their ccTLDs).

[47] *Id.*

[48] *See* SARROCCO, *supra* note 2, at 17 (noting that many e-mail addresses have no geographic identifier and even when messages are sent from an address with a ccTLD, that does not provide any indication about the location from which the message was sent).

[49] *Id.*

[49] *Id.*

[50] *Id.*

[51] *Id.*

[52] *See also* Sorkin, *supra* note 13, at 344–51. *See generally* YOKE & TAN, *supra* note 20.

mail technologies when they were first developed.[53] As the Internet has expanded and questionable conduct such as spam has grown with it, these security flaws have enabled the spam problem to persist.[54] The technical solutions being implemented are largely built to plug these security holes.[55]

Spam-fighting technologies can be roughly grouped into three forms.[56] First and perhaps most important are those efforts to combat spam at the originating e-mail server in order to prevent messages from ever being sent.[57] Second, there are systems that reside at the ISP of the e-mail recipient that try to stop the messages.[58] Lastly there are systems controlled by Internet users themselves that help block spam before they reach the user.[59]

1. Blocking Spam From the Originating Server

To stop mail at its origin point, ISPs must attempt to add layers of security to their e-mail servers.[60] The protocol, or technology standard, used to send most e-mails is known as SMTP, or Simple Mail Transfer Protocol.[61] SMTP servers, which are responsible for sending most e-mail, do not need to be authenticated in any way.[62] As a result, spammers can often take advantage of available open servers, or "open relays," and route their mail through these unsecured servers.[63] These spammers take advantage of other ISPs' servers without authorization, and because there is no authentication, the spammers can disguise their identities.[64] There are several solutions to this problem.[65] For example, if every ISP required some kind of outgoing authentication,

---

[53] *See, e.g.*, Sarrocco, *supra* note 2, at 5 ("the basic Internet architecture . . . is intrinsically insecure, allowing spammers to operate anonymously and to evade law enforcement").

[54] *Id.*

[55] Yoke & Tan, *supra* note 20, at 6 (noting that closing security loopholes can help resolve the spam problem).

[56] *See id.* at 4–5.

[57] *Id.*

[58] *Id.*

[59] *Id.*

[60] Yoke & Tan, *supra* note 20, at 5–6.

[61] For a more complete definition of the SMTP protocol, see Definition of SMTP, Webopedia, http://www.webopedia.com/TERM/S/SMTP.html (last visited Feb. 12, 2006).

[62] *See* Sarrocco, *supra* note 2, at 5.

[63] *See* Sorkin, *supra* note 13, at 339.

[64] *See* Sarrocco, *supra* note 2, at 13.

[65] *See, e.g.*, Yoke & Tan, *supra* note 20, at 5–7.

then ISPs would be able to track every spam message to a particular account and deactivate the account before more spam is sent.[66]

Another technical solution is to block a network communications port on computers and networks known as "Port 25."[67] Today, over 40% of all spam is sent, often via Port 25, by unwitting users whose computers have become spamming "zombies," after being infected with a virus.[68] If ISPs block this port from their networks, then they can limit the amount of spam being sent in this manner.[69]

Third, ISPs can limit the number of outgoing e-mails that can be sent by any one user.[70] This would permit users to send e-mails to a limited list of recipients, while stopping spam messages from being sent to thousands of people at a time.[71]

Lastly, many organizations have been developing authentication mechanisms that ensure that the name and e-mail address on an e-mail message indeed corresponds to the correct user.[72] Outgoing ISPs can confirm that e-mails are indeed sent from their customers and are not fraudulent, so incoming ISPs can then route them efficiently.[73] This, however, raises several problems.[74] These authentication systems have not been standardized, so there is no common way for users to authenticate themselves or for recipients to confirm that authentication.[75] The other problem is that legitimate users, who have not, for whatever reason, been able to authenticate their e-mail address, may find that their messages are rejected by recipients.[76]

---

[66] *Id.* at 6–7; *cf.* Magee, *supra* note 6, at 343–44 (discussing efforts by ISPs to prevent spam by including anti-spam terms in their user contracts but noting that the lack of authentication makes it difficult to enforce these contracts).

[67] Yoke & Tan, *supra* note 20, at 5. For a discussion of network ports and related terminology, see Port (computing), http://en.wikipedia.org/w/index.php?title=Port_(computing)&oldid=41985982 (last visited March 3, 2006).

[68] Yoke & Tan, *supra* note 20, at 5*; see also* Gross, *supra* note 38.

[69] Yoke & Tan, *supra* note 20, at 5.

[70] *Id.* at 6.

[71] *Id.*

[72] *Id.*

[73] *Id.* at 6–7.

[74] *See infra* notes 75–76 and accompanying text.

[75] Yoke & Tan, *supra* note 20, at 7 (listing the various proposed authentication methods).

[76] *Cf. id.* at 5 (noting that similar solutions, such as Port 25 blocking, can have the effect of blocking legitimate e-mails).

2. Blocking Spam by the Receiving ISP

At the receiving ISP, several options are available as well.[77] One of the more controversial options is to implement a reputation system.[78] These systems rate incoming mail servers by their reputations for sending spam.[79] If an ISP is known to be the source of spam, a receiving ISP can simply block all e-mail traffic from that ISP.[80] The risk here is that not all e-mail traffic from that ISP is likely to be spam and many legitimate e-mails could be blocked.[81] One form of these reputation systems are "blacklists" and "whitelists," which companies compile to list e-mail addresses, domains, and IP addresses that are deemed either consistent spammers or safe senders, respectively.[82] Blacklists and whitelists have been effective at blocking some spam and are shared with ISPs to use in conjunction with other spam-fighting methods.[83]

3. End-user Spam Filtering Techniques

Lastly, there are end-user based filtering mechanisms.[84] These can be both static and Bayesian.[85] Static filters are simply lists of e-mail addresses from which e-mails are automatically deleted.[86] Bayesian filtering provides a more robust solution that gradually "learns" what a user regards as spam.[87] The problem with these systems is that they tend to generate false positives and mark legitimate mail as spam, while spammers are constantly working to beat their algorithms.[88] Both of these filtering technologies are widely used in all of the major e-mail services today.[89]

---

[77] *See id.* at 5–11.

[78] *Id.* at 9–10.

[79] *Id.*

[80] *Id.*

[81] Sarrocco, *supra* note 2, at 12.

[82] Yoke & Tan, *supra* note 20, at 9–10.

[83] *See* The Spamhaus Project, http://www.spamhaus.org (last visited Mar. 7, 2006) (providing blacklists, whitelists, and other anti-spam services to ISPs); *see also* John Levine, *How to Stop Spam*, CircleID, Jan. 24, 2005, http://www.circleid.com/posts/how_to_stop_spam/.

[84] Yoke & Tan, *supra* note 20, at 11–13.

[85] *Id.* For additional background on Bayesian spam filtering, see Bayesian Filter, http://whatis.techtarget.com/definition/0,289893,sid9_gci957306,00.html (last visited Mar. 8, 2006).

[86] Yoke & Tan, *supra* note 20, at 11–13.

[87] *Id.*

[88] *Id.* at 14 (noting the false positive risk and that spammers try to avoid filters by purposely misspelling words in their spam).

[89] Yoke & Tan, *supra* note 20, at 13.

E. *National Legislative Approaches to Fighting Spam*

While technical solutions have proliferated, many national governments, and indeed much of the international community, believe that the fight against spam cannot be adequately fought without legislation and enforcement.[90] As a result, many countries have enacted anti-spam laws.[91] These laws diverge, however, in their definitions of spam and their methods of enforcement.[92] These differences may prove to make international cooperation difficult in the future.[93] There are many different models for enforcing spam laws, so countries have enacted laws with any combination of criminal sanctions, civil actions brought by their governments, or private rights of actions that may be brought by individuals or ISPs.[94]

There are, however, some commonalities to most of these laws.[95] Most consider unsolicited e-mail to be illegal when it conceals the sender's identity, uses a third party's domain name without permission, or provides misleading information in the subject line of the e-mail.[96] In general, these laws either use an opt-in approach, in which prior authorization is required, or an opt-out approach, in which the recipient can opt-out of future messages.[97] Many of the laws require senders to clearly and accurately identify themselves as well.[98]

One such law is the CAN-SPAM Act, which the U.S. Congress enacted in 2003.[99] The Act preempted several state spam laws that had

---

[90] *See* HORTON, *supra* note 2, at ¶ 23. *See generally* MATTHEW B. PRINCE, HOW TO CRAFT AN EFFECTIVE ANTI-SPAM LAW (2004), http://www.itu.int/osg/spu/spam/contributions/Background%20Paper_How%20to%20craft%20and%20effective%20anti-spam%20law.pdf (recommending how legislation and enforcement can be more effective).

[91] *See generally* INT'L TELECOMMS. UNION, ITU SURVEY ON ANTI-SPAM LEGISLATION WORLDWIDE (2005), *available at* http://www.itu.int/osg/spu/spam/legislation/Background_Paper_ITU_Bueti_Survey.pdf; INT'L TELECOMMS. UNION, ANNEX I: WORLDWIDE AUTHORITIES AND LEGISLATIVE FRAMEWORKS ADDRESSING SPAM [DRAFT IN PROGRESS] (2004), *available at* http://www.itu.int/osg/spu/spam/contributions/Background%20Paper_Building%20frameworks%20for%20Intl%20Cooperation_Annex%201.pdf [hereinafter WORLD-WIDE AUTHORITIES] (reviewing several countries' spam laws).

[92] HORTON, *supra* note 2, at ¶ 26 (noting that there is little agreement across jurisdictions as to what anti-spam laws prohibit).

[93] *Id.*

[94] *See* PRINCE, *supra* note 90, at 7-8; SARROCCO, *supra* note 2, at 14.

[95] *See* SARROCCO, *supra* note 2, at 14.

[96] *Id.*

[97] *Id.*

[98] *Id.*

[99] Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003, 15 U.S.C. §§ 7701–7713, 18 U.S.C. § 1037 (2006).

attempted to solve the problem.[100] The law follows an "opt-out" policy, permitting unsolicited bulk email as long as the messages are not misleading or fraudulent, accurately represent the purpose of the message, and provide recipients an opt-out option.[101] This opt-out mechanism must work and there must be a legitimate e-mail address to which users can send messages to unsubscribe.[102] This is meant to address the problem of spammers providing ineffective or fraudulent methods of opting out.[103]

The U.S. Congress identifies spam as messages that: (1) are sent through a server without authorization; (2) are sent via "zombie" computers with the intent to deceive recipients or ISPs; (3) have falsified header information, such as "from," "to," or tracking information; (4) that falsify the identity of the sender; or (5) otherwise falsely represent the sender.[104]

The CAN-SPAM Act provides for criminal enforcement by the Federal Trade Commission (FTC) and provides a civil cause of action for state attorneys general and ISPs to sue spammers.[105] Several prosecutions and civil actions were brought pursuant to the CAN-SPAM Act in its first year of enactment.[106] The CAN-SPAM Act, however, received much criticism for its opt-out approach, which effectively permits spammers to send one e-mail to anyone, provided that there is an opt-out mechanism.[107] Studies have shown no noticeable decline of spam since the Act went into effect.[108]

Elsewhere, Australia passed its 2003 Spam Act, which went into effect in April 2004.[109] This is an opt-in regime, forbidding spam from being sent even once, and providing primarily for civil damages

---

[100] 15 U.S.C. § 7707(b)(1). *See generally* Magee, *supra* note 6, at 356–58 (providing an overview of pre-CAN-SPAM state laws).

[101] 15 U.S.C § 7704(a).

[102] *Id.*

[103] *See id.* § 7701(a)(9).

[104] *See* 18 U.S.C. § 1037(a).

[105] 15 U.S.C. § 7706(d), (f), (g).

[106] *See* Horton, *supra* note 2, ¶ 27; David Cohen, *Spam Is Finally a Crime,* Wired News, Nov. 4, 2004, http://www.wired.com/news/business/0,1367,65594,00.html.

[107] *See* Tom Zeller, Jr., *Law Barring Junk E-Mail Allows a Flood Instead,* N.Y. Times, Feb. 1, 2005, at A1; Spamhaus, Spamhaus Position on CAN-SPAM Act of 2003 (S.877 / HR 2214), http://www.spamhaus.org/position/CAN-SPAM_Act_2003.html (last visited Mar. 7, 2006) ("Spamhaus sees the introduction of the CAN-SPAM Act of 2003 (S.877/HR 2214) as a serious failure of the United States government to understand the Spam problem.").

[108] *See* Zeller, *supra* note 107.

[109] Worldwide Authorities, *supra* note 91, at 3.

against spammers.[110] Similarly, the European Union has also enacted opt-in spam legislation.[111] Despite the stronger regime, critics argue that because most spam originates outside of Europe, the law lacks enforcement power.[112]

F. *International Cooperation on Spam*

In recent years, many countries have recognized that without international cooperation, their domestic anti-spam legislation is insufficient.[113] As a result, several countries have begun cooperating on anti-spam initiatives.[114] Australia has made international spam cooperation a key element in a multi-tiered strategy to combat spam.[115] Australia has proposed a flexible approach to cooperation in which different countries (1) introduce domestic spam legislation that is reasonably coordinated and (2) commit to respond effectively to information about spammers beyond their borders.[116] Australia has proposed and entered into a few bilateral and multilateral agreements dealing with spam.[117]

The European Union has also proposed a system of cooperation to combat spam.[118] It has proposed a series of coordinated actions that member states should implement, including effective enforcement of laws and national strategies to ensure communications between the various regulatory agencies.[119] It also suggests using or creating a "liaison mechanism" to help support cross-border spam enforcement.[120]

The United States, the United Kingdom, and Australia recently entered into a Memorandum of Understanding (MoU) agreeing to work together to combat spam.[121] This agreement committed the coun-

---

[110] John Haydon, Multi-lateral and Bi-lateral Cooperation: the Australian Approach 1–2 (2004), *available at* http://www.itu.int/osg/spu/spam/presentations/ HAYDON_Session%208.ppt.

[111] Worldwide Authorities, *supra* note 91, at 5.

[112] *European Anti-Spam Laws Lack Bite*, BBC News, Apr. 28, 2004, http://news.bbc.co.uk/2/hi/technology/3666585.stm.

[113] Gérard, *supra* note 8, at 4 (noting the "crucial role for multilateral and bilateral cooperation").

[114] *See* Haydon, *supra* note 110, at 4.

[115] *Id.* at 2.

[116] *Id.* at 2–3.

[117] *Id.* at 4.

[118] Sarrocco, *supra* note 2, at 15.

[119] *See* Gérard, *supra* note 8, at 10–12.

[120] *Id.*

[121] Memorandum Of Understanding on Mutual Enforcement Assistance in Commercial E-mail Matters Among the Following Agencies of the United States, the United King-

tries' respective spam-fighting agencies to working together to enforce each country's spam laws.[122] Recognizing that "[i]llegal spam does not respect national boundaries," the FTC agreed to work closely with the United Kingdom's Secretary of State for Trade and Industry, Australia's Competition and Consumer Commission, and the Australian Communications Authority to share research, knowledge, technical expertise, evidence, and other enforcement information.[123] The MoU respects the different spam laws in each country, with their different definitions of spam, yet it encourages each country to cooperate in enforcing the laws in the other countries.[124] It also recognizes that it is impossible to cooperate on every spam case, so it recommends cooperation on only the most significant or most damaging spam cases.[125]

Perhaps the most significant effort at internationalizing the spam problem began with a global summit of the United Nations, known as the World Summit on the Information Society (WSIS).[126] This summit took place over the course of a few years, first meeting in December, 2003 in Geneva and meeting again in November, 2005 in Tunis.[127] The summit was sponsored by the International Telecommunications Union (ITU), which is a UN body charged with regulating parts of the international telecommunications infrastructure.[128]

The summit arose out of UN General Assembly Resolution 56/183, which, as part of the Millennium Declaration initiative to rid the world of poverty, called for a multi-part meeting to promote access to the Internet and information across the world.[129] WSIS involved governments, technology companies, and other public interest organizations in discussions addressing a wide range of issues, from how

---

dom, and Australia: the United States Federal Trade Commission, the United Kingdom's Office of Fair Trading, the United Kingdom's Information Commissioner, Her Majesty's Secretary of State for Trade and Industry in the United Kingdom, the Australian Competition and Consumer Commission, and the Australian Communications Authority, June 30, 2004, *available at* http://www.ftc.gov/os/2004/07/040630spammoutext.pdf [hereinafter MoU].

[122] Press Release, Federal Trade Commission, Consumer Protection Cops Join Forces to Fight Illegal Spam: Six Agencies on Three Continents Will Leverage Law Enforcement Efforts (July 2, 2004), *available at* http://www.ftc.gov/opa/2004/07/mou.htm.

[123] *Id.*

[124] *See* MoU, *supra* note 121, at 1.

[125] MoU, *supra* note 121, at 5.

[126] *See* Grossman, *supra* note 9. *See generally* KLEIN, *supra* note 10.

[127] Grossman, *supra* note 9.

[128] KLEIN, *supra* note 10, at 2; Hans Klein, *The Internet: Place, Property, or Thing—All or None of the Above?*, 55 MERCER L. REV. 947, 949 (2004) [hereinafter Klein, *The Internet*].

[129] G.A. Res. 56/183, U.N. GAOR, 56th Sess., U.N. Doc. A/RES/56/183 (Jan. 31, 2002).

to "govern" the Internet, to spam, to increasing access to communications technologies around the world.[130]

Two concluding documents from the Geneva phase of WSIS, the Declaration of Principles and the Plan of Action, cited spam as a problem requiring international attention and committed the parties to working together to solve this problem.[131] After the Geneva phase, the WSIS convened a Thematic Meeting on Countering Spam.[132] This meeting gathered governments, consumer groups, ISPs, nongovernmental organizations, and experts from the software and Internet technology industries to discuss the latest efforts in combating spam.[133] The parties to the meeting made several political, legal, and technical recommendations on how to combat spam and also provided an overview of the current state of global anti-spam efforts.[134] Finally, the Tunis phase produced even more statements of international commitment to fight spam.[135]

G. *Brief Overview of Internet Governance*

Another one of the focus areas of WSIS was a global discussion of "Internet governance."[136] Although it does not have a specific definition, at its heart, Internet governance includes the private organizations, governments, treaty organizations, and other bodies that, to some degree, govern the Internet.[137] Because the Internet is borderless and has so many constituencies, national governments have a limited role in Internet governance, which they share with many other institutions.[138] For this reason, there is much debate about

---

[130] *Id.*; Grossman, *supra* note 9.

[131] Declaration of Principles, *supra* note 11, ¶ 37; World Summit on the Info. Society, Plan of Action ¶ 12(d) (WSIS Doc. WSIS-03/GENEVA/DOC/0005) (2003), *available at* http://www.itu.int/dms_pub/itu-s/md/03/wsis/doc/S03-WSIS-DOC-0005!!PDF-E.pdf.

[132] *See* Horton, *supra* note 2, ¶ 1.

[133] *Id.* ¶ 4.

[134] *See id.* ¶¶ 4, 8.

[135] *See generally* Deborah Hurley, Int'l Telecomms. Union, ITU WSIS Thematic Meeting on Cybersecurity, Chairman's Report (2005) ¶¶ 6–35, *available at* http://www.itu.int/osg/spu/cybersecurity/chairmansreport.pdf [hereinafter Cybersecurity Report) (reviewing the results of the cybersecurity meeting); Tunis Agenda, *supra* note 11, ¶ 41 (expressing support for the fight against spam at the end of the Tunis phase).

[136] Declaration of Principles, *supra* note 11, ¶ 50 (asking the UN to set up a working group for Internet governance).

[137] *See* Milton Mueller et al., *Making Sense of "Internet Governance": Defining Principles and Norms in a Policy Context*, *in* Internet Governance, *supra* note 45, at 100, 101–03.

[138] *Id.*

whether there should be any formal governing structure and how effective such a structure can be.[139]

At the heart of this debate is the Internet Corporation for Assigned Names and Numbers (ICANN), which was established in the United States as the organization that controls the core domain name system by providing ISPs and companies with their Internet domain names.[140] ICANN serves as a quasi-international body, which manages the domain name distribution and conflict resolution process for the entire Internet.[141] ICANN is incorporated under U.S. contract law and is subject to U.S. law.[142] Many other countries believe that a United Nations body, such as the ITU, should govern such a critical aspect of the Internet and have pushed towards this result in the WSIS context.[143]

At this point, there is no central governance institution concerned with the fight against spam, but the debates on Internet governance in general and ICANN in particular may inform the debate about the feasibility of such an institution.[144]

II. Discussion

International efforts to combat spam present many difficult issues.[145] At the same time, however, there is consensus that spam is a problem that needs an international response.[146] The challenge, therefore, is in finding the common ground on which to move forward. [147]

---

[139] *See generally* Declan McCullagh, *Internet Showdown in Tunis*, Cnet News.com, Nov. 11, 2005, http://news.com.com/Internet+showdown+in+Tunis/2008-1012_3-5945200.html; Markus Kummer, *The Results of the WSIS Negotiations on Internet Governance, in* Internet Governance, *supra* note 45, at 53, 53–55.

[140] *See generally* Wolfgang Kleinwächter, *Beyond ICANN vs. ITU: Will WSIS Open New Territory for Internet Governance?, in* Internet Governance, *supra* note 45, at 31, 32, 38–40.

[141] Klein, *The Internet*, *supra* note 128, at 950–53.

[142] *Id.* at 948–51.

[143] *Id.* at 959–61.

[144] Kleinwächter, *supra* note 140, at 32 (noting that in the early stages of WSIS, some governments wanted to expand the concept of Internet governance to include many Internet related issues such as spam and illegal content and to have an international institution such as the ITU to take over this initiative).

[145] *See generally* Horton, *supra* note 2, ¶¶ 23–35.

[146] *See, e.g.*, Declaration of Principles, *supra* note 11, ¶ 37; Michelle Delio, *Spam Gets Its Claws in the U.N.*, Wired News, Mar. 28, 2004, http://www.wired.com/news/politics/0,1283,62824,00.html.

[147] *See* Sarrocco, *supra* note 2, at 18.

A. *Freedom of Speech, Regulation of Commerce, and Spam Definitions*

One of the threshold issues in the fight against spam is how to define it.[148] It may be tempting to simply call all unwanted e-mail spam, or to take an approach similar to the one Justice Potter Stewart used to define pornography ("I know it when I see it."),[149] but a more specific definition is necessary to create enforceable spam laws.[150] Some say that all unsolicited bulk e-mail (UBE) should be considered spam, while others suggest that the messages must also be commercial in nature.[151] The latter messages are known as unsolicited Commercial E-mail (UCE).[152] Still others argue that to be considered spam, a message must have no "unsubscribe" mechanism and must somehow disguise its sender or its intent with fraudulent or misleading header information.[153]

Underlying these various definitions is a range of ideas behind what is an appropriate use of Internet resources.[154] Most people agree that for a message to be considered spam, it must be bulk in nature.[155] This is because the primary problem of spam is that it consumes users' time and bandwidth.[156] Of course, the other key component is that the message be unsolicited.[157]

A key debate, therefore, is whether noncommercial bulk e-mails should be considered spam.[158] These include charitable fundraising solicitations, political ads, chain letters, and other such messages.[159] Those who would prefer to limit the scope of "spam" to UCE argue that private and public spam enforcement should primarily punish those who use spam for profitable gain.[160] Those who support broader UBE restrictions argue that since the harm is the same for any spam mes-

---

[148] Sorkin, *supra* note 13, at 326–36.

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

[150] *See* Sorkin, *supra* note 13, at 327.

[151] *Compare* Sorkin, *supra* note 13, at 327–35, *with* Spamhaus, The Definition of Spam, http://www.spamhaus.org/definition.html (last visited Mar. 7, 2006).

[152] Sorkin, *supra* note 13, at 327–35.

[153] *Id.*; 18 U.S.C. § 1037(a) (defining elements of fraud in connection with commercial e-mail).

[154] Magee, *supra* note 6, at 338 (noting that spam regulation presents a clear contradiction between business interests and those of private individuals who do not want to receive spam).

[155] Sorkin, *supra* note 13, at 330–31.

[156] *Id.*

[157] *Id.* at 328–29.

[158] *Id.* at 333.

[159] *Id.*

[160] Sorkin, *supra* note 13, at 334.

sage, they should all be combated.[161] The United States, however, has constitutional restrictions against regulating non-commercial speech and is unable to broadly regulate UBE.[162]

The issue of how to define spam, which necessarily touches upon the fine distinction between legitimate commercial speech and unwanted spam, is a difficult one.[163] It presents a complex policy question about how much commercial speech is appropriate and at what point it intrudes on the rights of others.[164]

In the United States, the First Amendment restricts Congress's ability to pass enforceable anti-spam legislation.[165] The Supreme Court held in *Central Hudson Gas & Electric Co. v. Public Service Commission of New York* that the First Amendment protects commercial speech from regulation, provided that it is otherwise lawful and not misleading.[166] If the speech meets these criteria, then any regulation of it must directly advance a substantial governmental interest and must not be more extensive than necessary to meet that objective.[167] In developing the CAN-SPAM Act, Congress could therefore only narrowly regulate bulk e-mail messages that are not misleading or otherwise illegal.[168] To regulate these more legitimate commercial e-mails, Congress needed to assert that the law was necessary to serve a substantial government interest.[169] Congress reasoned that even non-misleading or illegal spam must be regulated to preserve "the viability of e-mail as a medium of communication" because "there is a real danger that this medium will be rendered useless without regulation."[170] Considering the massive amounts of spam relative to legitimate e-mail, Congress was able to find a substantial government purpose to meet the *Central Hudson* test.[171]

---

[161] *Id.* at 335.

[162] *See generally* Marc Simon, *The CAN-SPAM Act of 2003: Is Congressional Regulation of Unsolicited Commercial E-Mail Constitutional?*, 4 J. High Tech. L. 85 (2004).

[163] *See* Magee, *supra* note 6, at 338–39.

[164] *See id.*

[165] *See id.* at 358–60.

[166] 447 U.S. 557, 566 (1980).

[167] *Id.*

[168] *See generally* Simon, *supra* note 162 (providing a complete constitutional analysis of the CAN-SPAM Act).

[169] Magee, *supra* note 6, at 359.

[170] Michael A. Fisher, *The Right to Spam? Regulating Electronic Junk Mail,* 23 Colum.-VLA J.L. & Arts 363, 409–10 (2000).

[171] *See* Simon, *supra* note 162, at 95; Magee, *supra* note 6, at 359.

Nonetheless, to meet the proportionality requirement, the CAN-SPAM Act needed to rely on an opt-out approach to UBE.[172] This permitted "legitimate" e-mail marketing messages to be sent once, as long as consumers could opt out of further messages.[173] Although an opt-in approach would probably be a more effective anti-spam regime, it could very well be found to be disproportionate in that it would block many mailings that could be considered protected commercial speech.[174]

While the CAN-SPAM Act has a lenient opt-out policy to conform to U.S. law, it does set some standards for what is acceptable spam and what is not, including e-mail with forged identities, fraudulent schemes, viruses, and those without reliable opt-out mechanisms.[175]

These basic rules roughly correspond to spam laws in other countries, even if those countries have stricter, opt-in legislation.[176] Nonetheless, these two approaches do present a problem in creating any enforceable international spam regime.[177] If the international community were to adopt a multilateral agreement on spam, it may be forced to adopt an opt-out approach, which is the lowest common denominator approach to national spam laws.[178] Though this approach would be weaker than the existing laws in many countries, this may be necessary to set minimum enforcement standards that all countries can accept.[179] If it were to adopt a stricter opt-in approach, countries such as the United States may have to reject it due to do-

---

[172] *See* Jeffrey D. Sullivan & Michael B. De Leeuw, *Spam After Can-Spam: How Inconsistent Thinking Has Made a Hash Out of Unsolicited Commercial E-Mail Policy,* 20 Santa Clara Computer & High Tech. L.J. 887, 893 (2004) (noting that Congress never seriously considered an opt-in spam policy partially due to First Amendment concerns).

[173] *See* Prince, *supra* note 90, at 3 (discussing the commercial speech rationales behind opt-out policies).

[174] *See id.* (noting direct marketing statistics supporting the argument that an opt-in approach could "unreasonably burden legitimate businesses").

[175] 15 U.S.C. § 7704(a)(5) (providing that, for UCE to be lawful, it must include a valid, working opt-out mechanism, valid postal address of the sender, and "clear and conspicuous identification that the message is an advertisement or solicitation"); 18 U.S.C. § 1037(a) (criminal prohibition against the use of "zombies" and falsified domain names to send UCE).

[176] *See generally* Worldwide Authorities, *supra* note 91.

[177] *See* Sarrocco, *supra* note 2, at 16 ("The harmonization of legislative approaches to spam between different jurisdictions from which an e-mail user is likely to receive spam would be crucial in order to properly tackle the problem.").

[178] *See id.*

[179] *See id.* at 16.

mestic constitutional grounds.[180] Since the United States produces the lion's share of global spam, this problem could render such an international cooperation effort useless.[181]

B. *Internet Governance Debate*

Another challenge in developing a global solution to the spam problem involves the question of whether the Internet can or should be governed, and if so, by whom.[182]

Some scholars wonder if it is possible to govern the Internet or if this would even be beneficial.[183] Some say any attempts at formal governance are futile since the Internet is such a huge, seemingly uncontrollable network.[184] They argue that because the Internet spans borders, there is really no government or institution that can possibly regulate it.[185] Even if regulation were possible, these scholars fear that too much control could risk stifling the open communication, entrepreneurship, and inherently democratic virtues of the Internet.[186] Their concern is that too much intervention in the Internet could stifle commerce by cutting back on new innovations, and could impose the social mores of one group on the global Internet community.[187]

Nonetheless, several organizations play some Internet governance roles already.[188] Most prominent among these is ICANN, which monitors the domain name system and is the ultimate authority behind the naming conventions on the Internet.[189] ICANN works to establish contract-based rules to resolve public policy domain problems such as copyright and trademark infringement issues among domain owners.[190]

---

[180] *See* Sullivan & De Leeuw, *supra* note 172, at 893. *See generally* Adam Zitter, Note, *Good Laws for Junk Fax? Government Regulation of Unsolicited Solicitations,* 72 FORDHAM L. REV. 2767 (2004) (discussing the constitutionality of opt-in and opt-out systems).

[181] Cynthia L. Webb, *There's No Spam Like American Spam,* WASHINGTONPOST.COM, Feb 3, 2004, http://www.washingtonpost.com/ac2/wp-dyn/A8344-2004Feb3?language=printer (noting that 80% of European spam "is in English and 80% claims North America as its point of origin").

[182] *See, e.g.*, Kleinwächter, *supra* note 140, at 31 (noting that Internet governance is "one of the most controversial issues" in WSIS).

[183] *See, e.g.,* Zoë Baird & Stefaan Verhuist, *A New Model for Global Internet Governance*, *in* INTERNET GOVERNANCE, *supra* note 45, at 58, 61.

[184] *Id.*

[185] *Id.*

[186] *See, e.g., id.* (arguing that too much government involvement in Internet governance can have the unintended consequence of stifling free speech).

[187] *Id.*

[188] Mueller et al., *supra* note 137, at 103.

[189] *Id.* at 102.

[190] *Id.*

Other national government institutions also regulate online commerce in their countries.[191] In addition, the World Intellectual Property Organization (WIPO) has created some standards for content over the Internet and has mandated that its member states create and enforce Internet-related intellectual property laws.[192]

Some private individuals, companies, and other organizations have played governance roles as well.[193] Standards bodies, for example, develop the protocols that are used on the Internet, such as for e-mail, the World Wide Web, and display technologies such as HTML.[194] ISPs, as the gateways to the Internet, have some control over the actions of Internet users.[195] With regard to spam, ISPs have the power to block e-mails from senders before they get to their targets.[196] So to some extent, technology developers, private ISPs, and users play more of a role in Internet governance than do the governmental bodies discussed above.[197] Some people argue that spam regulation should be primarily left up to the private sector, with its constant improvements in anti-spam technology.[198] They argue that spam legislation and enforcement takes too long, that the laws are redundant because existing laws already cover privacy and fraud, and that private technological solutions are already bearing fruit in the fight against spam.[199] They argue that there is no need for any public or private centralized authority to manage the Internet or to combat spam and instead argue for a decentralized, private form of governance.[200] Such a system, based on a "peer production" model, puts governance in the hands of end users, ISPs, and employers who run the local networks that people use.[201]

---

[191] *See id.* at 102–03.

[192] *Id.* at 103.

[193] *See infra* notes 194–97 and accompanying text.

[194] Robert E. Kahn, *Working Code and Rough Consensus: The Internet as Social Evolution, in* INTERNET GOVERNANCE, *supra* note 45, at 16, 18 (describing the role of standards bodies in gradually developing standards of behavior on the Internet).

[195] *See, e.g.* YOKE & TAN, *supra* note 20, at 4–6.

[196] *See* Levine, *supra* note 83.

[197] S*ee generally* LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE (1999) (discussing the role that private technology has in creating the de facto law of the Internet).

[198] *See* Rich Kulawiec, *10 Reasons Why Involving Government in Spam Control Is a Bad Idea,* CIRCLEID, Jul. 19, 2004, http://www.circleid.com/posts/10_reasons_why_involving_government_in_spam_control_is_a_bad_idea.

[199] *See id.*; *see also* Levine, *supra* note 83.

[200] *See* David R. Johnson, et al., *The Accountable Internet: Peer Production of Internet Governance,* 9 VA. J.L. & TECH. 9, ¶ 2 (2004), http://www.vjolt.net/vol9/issue3/v9i3_a09-Palfrey.pdf.

[201] *Id.* ¶¶ 39–40.

Sometimes, however, individuals need true "hard law" to fall back on, when private regulation is not sufficient.[202] In the spam context, this could happen when a purportedly legitimate spammer feels his free speech has been violated by an over-sensitive ISP that blocks his e-mail.[203] In this case, the spammer may want to pursue his claim in court under substantive law, as opposed to fighting directly with ISPs.[204]

Internet governance and spam regulation are therefore governed by a sort of partnership between private and public institutions.[205] The question remains, however, how to organize all of these parties to best combat the spam problem.[206]

As discussed in Part II, many foreign governments and institutions believe that the United Nations, or one of its constituent organizations such as the ITU, should have the ultimate authority over Internet governance.[207] They feel that American institutions such as ICANN do not represent global interests as well as a UN body would.[208] On the other hand, some scholars believe that UN management may lead to limitations on free speech on the Internet and spam policy, as non-democratic member states apply pressure for censorship policies.[209] Any international spam resolution must take into account this debate between private governance institutions, quasi-governmental institutions such as ICANN, and international treaty organizations such as ITU or WIPO.[210]

C. *Intergovernmental Cooperation & Enforcement Challenges*

Though in recent years the international community has urged multilateral cooperation in the fight against spam, many barriers to effective enforcement remain.[211] One challenge in developing a cooperation regime is that the fight against spam is a "horizontal" challenge affecting many different areas of the law, including "telecom-

---

[202] *See* Sorkin, *supra* note 13, at 343–44 (discussing the "problems with self-regulation").

[203] *See id.* at 349 (noting that ISP filters interfere with legitimate e-mail traffic).

[204] *See* Sarrocco, *supra* note 2, at 12.

[205] *See generally* Baird & Verhulst, *supra* note 183; Johnson, *supra* note 200.

[206] *See* Magee, *supra* note 6, at 378–79 (discussing some frameworks for a global system to combat spam).

[207] *See* Klein, *The Internet*, *supra* note 128, at 959–60.

[208] *Id.*

[209] *See* Bruce Levinson, *Preventing a New World Internet Order,* CircleID, Jan. 18, 2005, at http://www.circleid.com/posts/preventing_a_new_world_internet_order/.

[210] Magee, *supra* note 6, at 378–80.

[211] Sarrocco, *supra* note 2, at 18 (noting the jurisdictional challenges to international spam cooperation).

munications, trade, privacy, and consumer protection."[212] As a result, non-spam legislation, such as anti-fraud or privacy laws, often target spammers as much as laws that specifically target spam.[213] In addition, even when countries have spam-specific laws, the related enforcement powers can vary.[214] Many countries do not offer criminal sanctions against spammers and only offer civil fines, while others offer these sanctions as well as private causes of action by either individuals or ISPs.[215] It is therefore challenging to develop an international regime that is flexible enough to account for the differences in the relevant local laws that affect spam.[216]

Similarly, most countries have several regulatory bodies that are responsible for spam.[217] In the United States, for example, the FTC and state attorneys general both enforce spam laws.[218] In other countries, this authority is vested in multiple agencies; for example, in the United Kingdom, the Information Commissioner and the office of Fair Trading and Her Majesty's Secretary of State for Trade and Industry all have some authority in this area.[219]

Adding another layer of complexity to the problem, many countries do not yet have any spam-specific legislation and currently have no plans to develop it.[220] This further complicates any coordination efforts among various states.[221]

Another issue with spam coordination is the cost of investigating and enforcing spam laws.[222] Spammers have become very skilled at hiding their identities through the use of technology, which significantly increases the costs of enforcement.[223] Because there are so many spammers, this would require hundreds of spam prosecutions, which of course drives up the costs considerably.[224] Many countries will only be

---

[212] *Id.* at 14.

[213] *Id.*

[214] *See* PRINCE, *supra* note 90, at 7-8; SARROCCO, *supra* note 2, at 14. *See generally* WORLDWIDE AUTHORITIES, *supra* note 91 (providing a list of spam laws worldwide and their enforcement mechanisms).

[215] *Id.*

[216] *Id.* at 14–18.

[217] SARROCCO, *supra* note 2, at 17.

[218] *See id.*

[219] *Id.*

[220] *See generally* PETR PIŠKULA & JANA KLASCHKOVÁ, REPORT ON NON-OECD COUNTRIES' SPAM LEGISLATION 6–10 (2004), http://www.oecd.org/dataoecd/26/47/31861202.pdf.

[221] *See, e.g.*, GÉRARD, *supra* note 8, at 3 (arguing that the first step in international spam cooperation is to establish effective anti-spam legislation in every country).

[222] PRINCE, *supra* note 90, at 4 (discussing the costs of prosecuting spammers).

[223] *See id.* at 5.

[224] *See id.* at 4–5.

willing to cooperate in investigating or prosecuting spammers in cases where there are significant damages.[225] Countries have many more important ways of spending their resources than prosecuting spammers, unless the value of the prosecution is clear.[226] This presents the problem of defining exactly what kinds of spam, and how much of it, causes enough damage to warrant the expense of international cooperation.[227]

Any cooperation regime must also spell out exactly what information must be shared across borders and what the expectations are for each party.[228] The MoU between the United States, Australia and the United Kingdom may provide a starting point for a comprehensive cooperation mechanism.[229] Rather than defining spam or mandating any specific spam laws, it defers to the laws and institutions of the participating countries.[230] It commits the parties to help each other gather evidence, serve process, share technology, and otherwise coordinate in the battle against spam.[231] It further provides for a strict confidentiality system to preserve the privacy of the parties involved in any international spam investigation.[232] The MoU, however, is merely aspirational, in that it does not create any "binding obligations under international law or under the domestic laws of the Participants."[233]

While loose agreements such as the MoU may be helpful, in light of the discussions at the various WSIS meetings, perhaps a more forceful agreement can be negotiated to combat spam on a larger scale.[234] Just as there are already several multilateral Internet governance institutions such as ICANN and the WIPO, perhaps a new organization, with its authority provided for in a multilateral treaty, can be created with limited jurisdiction over spam enforcement and cooperation.[235]

III. Analysis

Though there are many challenges to improving international cooperation on spam, WSIS provided a forum where many stakeholders around the world could debate the problem and begin

---

[225] *Id.*
[226] *Id.*
[227] Prince, *supra* note 90, at 5.
[228] *See, e.g.,* MoU, *supra* note 121, at 4–5.
[229] *See generally id.*
[230] *Id.* at 2–4.
[231] *Id.* at 3.
[232] *Id.* at 8.
[233] MoU, *supra* note 121, at 10.
[234] *See* Horton, *supra* note 2, ¶ 32.
[235] *See id.*

to develop comprehensive solutions.[236] The various sessions of WSIS discussed the many issues of the spam problem, and brought to light many initiatives that are being tried around the world.[237] At the end of the Tunis phase of the summit, the parties agreed to "adopt a multi-pronged approach to counter spam that includes, *inter alia*, consumer and business education; appropriate legislation, law enforcement authorities, and tools; the continued development of technical and self-regulatory measures; best practices, and international cooperation."[238]

In light of this decision, the challenge before the international community is how to expand on the existing multi-pronged approaches that were discussed at WSIS, such as the MoU, and create a framework that enables truly global cooperation in the fight against spam.[239] Any cooperative system must be flexible enough to meet domestic constitutional requirements and effectively interrelate with domestic laws while being forceful enough to deter spammers at an international level.[240] At the same time, such a system must not stifle the innovative capabilities of the private sector, technology companies, and ISPs, who provide the critical front-line defense against spam.[241] The framework must also enhance international cooperation to enable investigation, prosecution, and civil lawsuits against spammers who take advantage of the global nature of the Internet.[242]

Perhaps the best way to balance the interests involved would be to create a multilateral treaty organization that strengthens and expands upon the MoU and other similar initiatives, while preserving their flexibility to account for jurisdictional differences.[243] Because of the

---

[236] *Cf.* Delio, *supra* note 146 (noting that spam is one topic at WSIS that "the entire world can agree on").

[237] *See, e.g.*, Cybersecurity Report, *supra* note 135, ¶¶ 25–29 (reviewing many international initiatives on combating spam).

[238] Tunis Agenda, *supra* note 11, ¶ 41.

[239] *See id.*

[240] *See, e.g.,* Haydon, *supra* note 110, at 2; Prince, *supra* note 90, at 2–3 (arguing for more forceful "action laws" as opposed to unenforceable "sentiment laws" expressing a concern with spam); Sarrocco, *supra* note 2, at 18. These "domestic laws" include both spam-specific laws and more general laws governing fraud and the like. *See id.*

[241] Org. for Econ. Co-operation & Dev., Directorate for Sci., Tech. and Indus., OECD Workshop on Spam: Report of the Workshop (OECD Doc. No. DSTI/CP/ICCP(2004)1) ¶ 48 (2004), *available at* http://www.oecd.org/dataoecd/55/32/31450810.pdf [hereinafter OECD Report] (noting that some technical self-regulation will always be critical in order to deal with spam from countries not part of this agreement or those without any formal spam laws).

[242] *See, e.g.,* Prince, *supra* note 90, at 7–8.

[243] *See, e.g.*, Horton, *supra* note 2, ¶ 32.

flexibility required to address the spam issue, the challenges posed by creating one organization that would govern international spam law and enforcement are probably insurmountable.[244] It would be advisable, therefore, to create a body with more modest goals.[245] This organization could be modeled after the WIPO or the World Heath Organization, which encourage cross-border cooperation in their respective areas of expertise. It would require its members to enact some kinds of spam legislation and to provide for a minimal amount of enforcement and international cooperation.[246] It could serve as a clearinghouse organization that funds technological and legal research and encourages nation-states to enter into multi-lateral agreements to help stop spam.[247] This body would not, however, follow the ICANN model in attempting to create binding law that could effectively be enforced in multiple jurisdictions; rather it would set minimum standards for membership and develop and encourage new ways of cross-border cooperation.[248]

A. *Addressing Constitutional & Definitional Questions*

For any international agreement on spam to work, it must require that member states enact spam laws that include a baseline definition of spam.[249] The definitional aspect is crucial, not only because it provides for a basic understanding of what is considered to be spam, but depending on how broadly spam is defined, it has the potential to implicate constitutional speech regulations.[250] Thus, to ensure that many countries participate, this definition may need to adopt a "lowest common denominator" approach and set a standard that will produce minimal constitutional challenges in countries like the United States.[251] Consequently, the minimal standard would likely have to be an "opt-out" approach.[252] The agreement can follow the

---

[244] *See supra* notes 240–42 and accompanying text.

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

[246] *See infra* notes 249–260 and accompanying text.

[247] *See infra* notes 275–279 and accompanying text.

[248] *See infra* notes 249-53, 260-262.

[249] *See* Sarrocco, *supra* note 2, at 16.

[250] *See supra* notes 163–171, 176–181 and accompanying text.

[251] *See supra* note 178 and accompanying text.

[252] *See id.* As has been discussed, any international spam agreement would probably fail without United States participation, since the United States produces, or is the target of, a large majority of global spam. *See* Webb, *supra* note 181.

lead of the MoU, however, and give member countries the flexibility to adopt stricter, opt-in regimes if they choose to do so.[253]

The opt-in/opt-out debate may not, in fact, be a major stumbling block for agreements.[254] Empirical evidence shows that the most successful prosecutions have arisen out of opt-out regimes, largely because it is very difficult to prove that a user has not opted in to receiving a particular message.[255] With this in mind, it may be more practical to adopt a seemingly lenient standard for spam enforcement.[256]

The minimum definition of spam can follow the lead of the EU Directive 2002/58/EC, which established some "basic rules" that define spam.[257] These rules would declare spam illegal if it is UCE (this would not encompass all UBE, however) and does not have a working opt-out mechanism.[258] In addition, any of the following items would qualify a message as illegal spam: (1) it contains fraudulent subject headers, sender addresses, sender domains, or sender identification; (2) it is misleading in its nature; (3) it is otherwise illegal under existing laws for fraud, trademark, copyright, or other regulatory areas, such as unlicensed pharmaceutical sales.[259]

B. *Resolving Enforcement Challenges*

This anti-spam organization would set standards for what spam crimes are worthy of international cooperation, and if these standards were met, it would mandate that member states cooperate to the fullest extent possible.[260] It would set a threshold, using such variables as (1) quantity of spam; (2) amount of money lost due to fraud or identity theft; (3) other laws breached.[261] Like the MoU, it would be flexible to enable cooperation regardless of the specific enforcement bodies in various countries.[262]

This organization would also create a system through which any state investigating a spammer that meets the above threshold can re-

---

[253] *See supra* notes 224–226 and accompanying text.

[254] PRINCE, *supra* note 90, at 3–4.

[255] *Id.*

[256] *Id.*

[257] GÉRARD, *supra* note 8, at 5.

[258] *Id.*; *See supra* notes 98–105 and accompanying text.

[259] GÉRARD, *supra* note 8, at 5; *see supra* notes 98–105 and accompanying text.

[260] *See* PRINCE, *supra* note 90, at 4–5 (noting that prosecutors are only willing and able to prosecute the most egregious spam); *see also* MoU, *supra* note 121, at 5.

[261] *See, e.g.,* MoU, *supra* note 121, at 5.

[262] *See id.* at 2–3.

quest that other states investigate individuals and servers located in their jurisdiction and, if necessary, serve process to the relevant parties.[263]

Additionally, as a result of the jurisdictional problems associated with identifying and locating spammers and investigating the servers used in sending spam, the agreement should require that member states establish laws asserting jurisdiction over domestic Internet activity as well as domains using their ccTLDs.[264] This would enable, for example, the United Kingdom to assert jurisdiction over all e-mails sent from the .uk domain, even if the message was not sent from, or even routed through, any servers in the country.[265] This way, if the United States wants to investigate a spammer who sent a message from a British server, or who used a .uk e-mail address, the United Kingdom government will have jurisdiction to investigate if it receives a request under the agreement from the United States.[266] At the same time, the treaty must be flexible enough to account for domestic privacy and confidentiality rules.[267]

The parties would need to determine whether international spam laws should, at a minimum, provide for civil or criminal enforcement, or both.[268] Prosecuting spammers can be exceedingly expensive, largely because it is so costly to investigate a spammer, and because so many must be prosecuted before a law can have any meaningful effect.[269] Perhaps it would be effective for a treaty to mandate that countries enable private parties, such as ISPs, to bring civil actions against spammers.[270] This would shift the financial burden away from government to the parties that are most affected by spam.[271] Given that some countries' spam laws provide only civil causes of action, the agreement may once again require a lowest common denominator approach and mandate only that member states provide

---

[263] *See, e.g., id.* at 5.

[264] *See* PRINCE, *supra* note 90, at 8. For a definition of ccTLDs, see *supra* note 46 and accompanying text.

[265] *See, e.g.*, PRINCE, *supra* note 90.

[266] *See, e.g.*, OECD REPORT, *supra* note 241, ¶ 51.

[267] *See* MoU, *supra* note 121, at 8.

[268] *See* PRINCE, *supra* note 90, at 4 (noting that Virginia has had success by permitting ISPs to sue spammers); *see also* 15 U.S.C. § 7706(d), (f), (g).

[269] *See* PRINCE, *supra* note 90, at 4–5.

[270] *See id.* at 4.

[271] *Id.*

for state-initiated civil actions, while enabling cooperation with those states that choose to impose criminal sanctions as well.[272]

Because spam touches so many areas of law, it may be very difficult to limit the scope of an anti-spam treaty to avoid interfering with existing law enforcement mechanisms that target other related crimes.[273] It is therefore important that the investigation and enforcement rules confine themselves to a narrow definition of spam, while relying on existing laws and agreements to combat other offenses.[274]

C. *Internet Governance and the Role of the Technology Industry*

This proposed spam agreement can attempt to strike a balance between those who feel that the Internet needs centralized authority and those who prefer a "peer production" model.[275] Perhaps this organization can help provide some technical leadership in the fight against spam, without mandating any specific technical solutions.[276] It could help lead the way by serving as a clearinghouse for spam technologies and a conduit for ISPs and policy makers around the world.[277] It would fund private research and development of anti-spam technologies and would be a central point of reference for governments and technology companies about the latest available standards to combat spam.[278] In order to encourage competition and innovation among competing technology providers, however, this organization would not mandate the use of any specific technologies.[279] It would, however, make short-term recommendations, based on empirical evidence, about what solutions have been shown to be successful and would encourage cooperation between ISPs, users, and technology companies to help root out the spam problem.[280]

This loose framework could provide guidance to those countries that need it the most, including the developing nations that are just beginning to invest in their Internet infrastructure.[281] At the same

---

[272] *See, e.g., supra* notes 214–216 and accompanying text.

[273] *See* Magee, *supra* note 6, at 378–80.

[274] *See, e.g., id.* at 378.

[275] *See supra* notes 198–201 and accompanying text.

[276] *See* Johnson, *supra* note 200, ¶¶ 39–43 (noting the value in decentralized decision-making).

[277] *Id.*

[278] *Id.*

[279] *See, e.g., id.* ¶ 46 (arguing that peer governance and competition is well suited for combating Internet security risks).

[280] *See, e.g.,* OECD Report, *supra* note 241, ¶ 54.

[281] *See* Developing Nations Contribution, *supra* note 4.

time, it would enable ISPs and other Internet companies to explore new technologies that help keep up with the spammers when they have the resources to experiment.[282]

This organization would also serve as a point of reference to help national governments educate users and ISPs about the threat of spam and how to avoid it.[283] This would help clarify spam-fighting strategies and best-practices for those countries that need it.[284]

The fight against spam does not need to be completely centralized, as the domain name system is currently managed by ICANN.[285] Instead, this new organization can allow governments and private institutions to deal with the problems in their own way, as long as certain minimum standards are met.[286] This solution could provide the centralized guidance that some countries need in their fight against spam while also keeping technical control decentralized, thereby quelling the fears that centralized authority will stifle free speech on the Internet.[287]

D. *Advantages of This Approach*

In general, this organization would provide for a flexible, multi-tiered approach to combat spam.[288] The first tier is action-oriented, in that it would mandate that member states enact spam laws, and commit themselves to cooperating in investigation and limited enforcement in the most egregious spam cases.[289] It would provide basic legal standards and provide a framework for international cooperation and either civil or criminal enforcement.[290]

The second tier would be to serve as a central point of contact in the war against spam, in its role as a promoter of new technologies and cooperation between governments, ISPs, corporations, and users.[291] This structure would balance the various issues in the Internet governance debate by continuing to promote technological standards and peer production to independently block spam, while providing a

---

[282] *Cf.* YOKE & TAN, *supra* note 20, at 3 (noting that technology solutions are an "arms race" between the technology companies and the spammers).

[283] OECD REPORT, *supra* note 241, ¶¶ 57–59.

[284] *Id.*

[285] *See supra* notes 189 and accompanying text.

[286] *See generally* Johnson, *supra* note 200.

[287] *See, e.g.,* Levinson, *supra* note 209.

[288] *See,* e.g. HORTON, *supra* note 2, ¶ 37.

[289] *See supra* notes 222-234 and accompanying text.

[290] *Id.*

[291] *See supra* notes 285-287 and accompanying text.

backstop for when these policies fail.[292] This system would not "create an international government for the Internet," as some fear; it would simply provide some basic standards for national governmental cooperation.[293]

Conclusion

As spam has continued to proliferate, the private sector, national governments, and the international community have sought innovative ways to combat the problem. It has become clear that a multi-tiered strategy that leverages the skills in all of these areas is critical to combat spam. New technologies and coordination among ISPs are a critical first step, and national governments can provide prosecution and other legal remedies to go after spammers who get past these technologies. Without international cooperation, however, spammers can avoid the reach of governments by sending their spam across borders.

WSIS brought all of the relevant parties together to begin resolving the spam problem. Now that the international community is united against spam, they have an opportunity to develop new ways of coordinating the fight. The international community should take this opportunity to negotiate a broad-ranging international agreement that takes advantage of the skills of all relevant parties, without interfering with the commercial rights of citizens or the sovereign prosecutorial power of individual states.

Several smaller coordination and enforcement agreements have been implemented so far, and in light of the commitments made at WSIS, the international community can strengthen them with a flexible international agreement that requires members to get more involved in the fight against spam. At the same time, the organization created by this agreement would serve as an important clearinghouse for educational materials and technology standards for all relevant parties to use in their efforts to eliminate the problem. There is no "silver bullet" that will eliminate spam, but with the right planning, the international community can develop a clear, coordinated, international strategy to combat spam now, while remaining flexible enough to adapt to evolving spam technologies in the future.

---

[292] *Id.*

[293] Johnson, *supra* note 200, ¶ 1.