Research Publication No. 2005-
October 2005

Stemming the International Tide of Spam: A Draft Model Law

John Palfrey

This paper can be downloaded without charge at:

The Berkman Center for Internet & Society Research Publication Series:
http://cyber.law.harvard.edu/publications

The Social Science Research Network Electronic Paper Collection:
http://papers.ssrn.com/abstract_id=XXXXXX

Executive Summary.

Spammers continue to run circles around the anti-spam police. Dozens of countries have anti-spam laws on the books, yet enforcement of the statutes is costly, infrequent, and rarely, if ever, has any meaningful net effect on the amount of spam sent and received the next day. Each enforcement action is complex, frequently involving multiple jurisdictions, and more expensive than most developing countries can afford to undertake. Anti-spam enforcement must take more innovative forms than simply the direct pursuit of individual spammers by over-burdened regulators. Most important, any anti-spam initiative must be pursued in the context of multiple modes of regulation, including law, technology, markets, and social norms. The least-intrusive, least-costly, and ultimately most effective anti-spam measures are relatively simple things that end-users can do to protect themselves, such as spam filters on e-mail clients. But these end-user controls alone have not solved the problem, for a variety of reasons, and, while preferable as a solution, there is no consensus to pursue an aggressive end-user education route as the answer. As the spam problem worsens, it is taking on increasingly troubling dimensions of fraud as well as threatening to undermine efforts in developing countries to provide access to citizens. Legislators and regulators believe that they are compelled to act against spam in the public interest.

This chapter primarily takes up the question of what – beyond coordinating with technologists and other countries' enforcement teams and educating consumers – legislators and regulators might consider by way of legal mechanisms. First, the paper takes up the elements that might be included in an anti-spam law. Second, the paper explores one alternative legal mechanism which might be built into an anti-spam strategy, the establishment of enforceable codes of conduct for Internet Service Providers (ISPs). ISPs should be encouraged to establish and enforce narrowly-drawn codes of conduct that prohibit their users from using that ISP as a source for spamming and related bad acts, such as spoofing and phishing, and not to enter into peering arrangements with ISPs that do not uphold similar codes of conduct. Rather than continue to rely upon chasing individual spammers, regulators in the most resource-constrained countries in particular would be more likely to succeed by working with and through the ISPs that are closer to the source of the problem, to their customers, and to the technology in question. The regulator's job would be to ensure that ISPs within their jurisdiction adopt adequate codes of conduct as a condition of their operating license and then to enforce adherence to those codes of conduct. The regulator can also play a role in sharing best practices among ISPs and making consumers aware of the good works of the best ISPs. While effectively just shifting the burden of some of the anti-spam enforcement to ISPs is not without clear drawbacks, and cannot alone succeed in stemming the tide of spam, such a policy has a far higher likelihood of success in the developing countries context than the anti-spam enforcement tactics employed to date.

I. Introduction.

The anti-spam laws enacted around the world to date have failed.[i] Almost in every instance, anti-spam statutes are directed at sanctioning spammers for their bad acts. An increasing number of jurisdictions, often at the country and the state level, have created such laws. Other jurisdictions use existing laws of general application – such as data protection, consumer protection, or anti-fraud legislation – to fight spam. In many cases, these laws miss their target entirely, with no perceptible impact on actual spammers. Often, too, the laws have negative side effects, in the form of transaction costs, administrative costs, and a chilling effect on legitimate senders of e-mail, whether or not in bulk. No matter what kind of law is in use, anti-spam laws

require well-conceived, targeted, and coordinated enforcement mechanisms to be effective. The enforcement of anti-spam laws involves investigations that almost invariably become complicated and expensive. This cost and complexity can present challenges for any country seeking to enforce anti-spam laws. Even the United States Federal Trade Commission, with its substantial resources relative to other agencies of its kind around the world, has brought only approximately 70 cases against spammers. For developing countries that have limited human and financial resources for such work, anti-spam laws can be rendered near meaningless because of the enforcement challenge. And while cross-border cooperation and enforcement is not only desirable, but essential to spam-fighting, the variety of spam laws and underlying legal systems on the books of various states makes collaboration extremely difficult. The challenge of fighting spam through law – to be sure only one of the potential modes of regulation – calls both for new thinking and increased emphasis on harmonization and collaboration.

A. The Problem.

The problem of spam is well established. The extent of the problem is plain to anyone who relies upon electronic messaging as a means of communication and who uses the Internet actively. Electronic mail, along with related forms of messaging such as blogging and SMS, has become an important and popular means of communication in cultures around the world. People and businesses the world over rely upon electronic messaging for a wide range of functions on a daily basis. These services are cheap, have global reach, and have played a key role in the development of e-commerce. The value of the many merits of electronic messaging are rendered obvious by the application's extraordinary global adoption rate, whether in the form of an e-mail client (such as Microsoft's Outlook, Eudora, Thunderbird, or others) or hosted services (such as Microsoft's Hotmail, WebBlaze, Yahoo! Mail, Google's Gmail, Wanadoo or Noos in France, and so forth).

But the openness that has made e-mail and its close cousins such tremendously easy ways to connect is also emerging as their downfall. A combination of economics, technologies, and norms of behavior online has made it such that there is nearly zero incremental cost to send spam, and a more-than-zero return on that investment for senders. The economics seem baffling: how can it possibly be economically worthwhile to send out the grammatically-challenged messages about low-cost VI*%GRA or ripped-off copies of software that most people ignore or never see, as they pile up in "junk mail" folders? Part of the answer is that since the cost of sending the marginal electronic message is so low, the response rate does not need to be very high. It turns out that enough people do respond, either by buying the product marketed illicitly or otherwise acting on the message's information (such as buying a "headed through the roof!" penny stock or giving up your social security number or bank PIN code, in the phishing context), to make the endeavor worthwhile to the spammer. The Business Software Alliance, for example, found that an astonishing 22 per cent of British consumers surveyed purchased software through spam.[ii] Rates for the other five countries surveyed by BSA were similarly high. Spam persists because it is a profitable undertaking. Absent a level of consumer education that would result in fewer people falling for the ruse, the risk and cost to the spammer associated with sending spam must rise if the problem is to be solved in a comprehensive manner.

Spammers and those who perpetrate related frauds take advantage of the broadly open network design to render e-mail costly to recipients or even nearly unusable for some businesses and consumers. The "extremely rapid growth" of spam[iii] has led to the enactment of more than 75 specific laws,[iv] such as the well-regarded Australian law, the United States' CAN-SPAM Act of

2003 and the thirty-seven state laws that it largely pre-empted, and comparable legislation in several dozen countries around the world.[v] These laws have, to date, failed to stop spam. Each major, credible report on this topic suggests that more than half of the e-mails sent today are spam, and some suggest that spam comprises between 70 and 90 per cent of all e-mails sent.[vi] The costs of this scourge are borne not by the spammers, but by those who run the network, those who pay the recipients to work, and those who receive the messages. Accounts vary somewhat in terms of rates of growth, but there is no persuasive evidence that the growth of spam has abated in the wake of anti-spam legislation.[vii] In fact, most indicators point in the other direction.[viii]

Spam is most profitably viewed not as an isolated nuisance, but in the context of cybersecurity. Spam is bad enough as a drain on productivity in the society at large and as a daily annoyance for many people when they wake up. Spam is enormously costly to Internet Service Providers (ISPs) and others who maintain the network at various levels. Meanwhile, its negative impact is growing by virtue of the bad things it brings with it. Spam is the preferred delivery mechanism for a range of Internet security threats: viruses, phishing, pharming, endless permutations of scams, and advance fee fraud.[ix] Spam is also harming the efforts of those in developing countries to persuade new users to begin to rely on digital communications.

The problem is exacerbated by the fact that spam has, to date, defied both extensive lawmaking and concerted efforts on the part of leading technologists and their companies. Arguably the world's most powerful technologist, Bill Gates, promised to lead the charge against spam and to end it within two years of the January 2004 World Economic Forum meeting in Davos, Switzerland, which today seems unlikely to occur.[x] Mr. Gates has not been alone, as most major, well-intentioned ISPs and e-mail service providers, along with many technology start-ups, have devoted many millions of dollars to date toward spam-fighting measures. Standards-bodies have sought to improve protocols to snag more spam. User education campaigns have been launched. And governments around the world have come together to enforce their spam laws and to coordinate, periodically, more effectively with one another. The problem continues despite these many efforts, suggesting that new solutions must emerge and that existing efforts must be better pursued and coordinated.

Some of the most effective recent efforts have been those lawsuits undertaken by ISPs under a private right of action in spam legislation. In the United States, the CAN-SPAM Act of 2003 enables ISPs to sue spammers directly. AOL, Microsoft, and Earthlink – very large-scale providers of electronic messaging services – have each brought actions under this statute, as well as under state computer crimes and common law statutes, which have resulted in multi-million-dollar judgments or settlements against "spam king-pins" who abuse their networks.[xi] Microsoft's $7 million judgment against Scott Richter may have put an end to one network of spamming that allegedly distributed more than 38 billion unsolicited messages per year.[xii] These lawsuits, though few and far between and limited to certain jurisdictions, represent a ray of hope that enforcement by ISPs, with help from customers, might get the job done against spam. The success of these efforts suggests that ISPs could become the most valuable players in the effort to end spam. The trick for lawmakers is how to create a fair, effective regulatory regime that takes advantage of the abilities and positioning of ISPs to help end spam without placing an undue burden on law-abiding companies.

B. A Model Law: One of Several Ways to End Spam.

The persistence of the spam problem has led policy-makers, technologists, academics, and many others to come up with a wide range of possible strategies for how to end spam. The least intrusive approach, most consonant with the end-to-end principle of network design, is to leave the work to the end-users, through simple technologies such as spam filters on e-mail clients. Emerging technologies such as authentication, accreditation, and identity management ought to help make user-level controls more effective over time.[xiii] Mr. Gates, at Davos in 2004, proposed three specific solutions that Microsoft was pursuing that would largely complement these user controls.[xiv] The most comprehensive of these proposals, in the fashion made famous by Lawrence Lessig of Stanford Law School, call for a combination of law, code, markets, and norms.[xv]

The chairman's report of the ITU Thematic Workshop on Countering Spam in 2004 contains a range of such proposals and suggests the intersection of these many methods of spam-fighting.[xvi] This comprehensive, five-part approach calls for a combination of:

- Strong, enforceable legislation;
- The continued development of technical measures;
- The establishment of meaningful industry partnerships, especially with Internet Service Providers, mobile carriers and direct marketing associations;
- The education of consumers and industry players about anti-spam measures and Internet security practices; and,
- International cooperation at the levels of government, industry, consumer, business and anti-spam groups, to allow a global and coordinated approach to the problem.

Virtually every major report on spam calls for a combination of approaches to end the spam problem, rather than a single "silver-bullet"-style solution. This chapter does not take up in detail each of these anti-spam tools, but rather focuses on legal strategies, with an emphasis on those of relevance to developing countries.

Regardless of which anti-spam strategy, or combination of strategies, one prefers as a primary solution, anti-spam laws are today perceived to be a necessary tool that all countries may wish to consider adopting. If for no other reason, adoption of an anti-spam statute helps to facilitate international cooperation in combating spam. Even the most ardent supporters of user-based, technology, or market solutions to spam tend to agree that governments have a role to play in tracking down and punishing the worst offenders, such as those who use spamming as a means to defraud unsuspecting users. As prominent cyberlaw expert Michael Geist notes, we are in the "third phase" of anti-spam law development, where the anti-spam issue is increasingly viewed as "an enforcement problem that requires significant government involvement at both the national and international level."[xvii] The existence of interoperable anti-spam laws creates the common baseline essential to coordinated enforcement. While a developing country may not have the necessary resources to enforce its anti-spam legislation alone, there may be anti-spam activities of an international nature in which two or more countries may cooperate to shut down the worst spammers. A country with experience enforcing anti-spam legislation may wish to provide

human resources to conduct an anti-spam investigation and enforcement action that leads to another country. In the absence of anti-spam legislation, however, such international cooperation is not possible on a systemic basis. Anti-spam laws are increasingly viewed as one of several necessary tools for most countries.

Spam is arguably a bigger problem in developing countries, where anti-spam infrastructure is infrequently in place, than in wealthier countries, where anti-spam mechanisms are more robust. Many developing countries do not yet have anti-spam legislation.[xviii] Those that do often are constrained in their ability to devote the necessary resources to enforce these laws.[xix] The drain on the technical infrastructure, even if lighter in absolute terms, is relatively more costly in the developing country context. ISPs are frequently deluged by spikes in spam, which lead to network slowdowns and breakdowns.[xx] Many sending emails in developing countries do so from shared Internet connections and equipment, such as cyber cafés or other public access centers, and as such ordinarily rely on hosted email services with limits on inbox sizes. These customers complain that spam is tantamount to a denial of service since accessing email becomes too expensive if per-minute charges paid to cyber café owners are consumed by cleaning spam from their inboxes. Even worse, legitimate emails are bounced because the limited space of their inboxes is consumed by spam. Representatives of developing countries point to the fact that most, or at least much, spam still comes from the United States and other wealthy countries and that little support in terms of resources to fight the problem locally have been forthcoming. In addition, representatives of developing countries have argued that the resources of regional bodies such as the OECD are not available to developing countries consistently, leaving developing countries at a comparative disadvantage in terms of being able to do something about spam.

The answer for developing countries is not simply to enact an anti-spam law akin to those passed elsewhere, as such an approach is unlikely to have a perceptible effect. Anti-spam laws aimed at sanctioning spammers, even if codified, may be little used in developing countries. This paper takes up the challenge of introducing the outline of a model anti-spam law that might be tailored to usage in a developing countries context where no anti-spam law yet exists. This paper further takes up the question of whether there are other steps regulators in developing countries could take to combat spam, such as an enforceable code of conduct system related to a country's ISPs.[xxi]

C. An Alternative Mechanism: Enforceable Codes of Conduct.

This paper explores the possibility of introducing into anti-spam legislation, particularly in developing countries, the requirement that ISPs establish a code of conduct relative to spam-related activity. The proposal also calls for provisions in the statute that empower the regulator to enforce that code against the ISP in the event of material breach of the code.[xxii]

Such a proposal cuts – jarringly – across the grain of most Internet regulation to date. ISPs, which are essential players in terms of development of ICT-powered economies, have generally been left alone by legislatures, administrative agencies, and judges. Though licensed and overseen by regulators in some contexts, ISPs have tended to enjoy broad immunity from prosecution related to the bad acts of people on and via their networks. Such a general posture has served development of the global network of networks very well; notwithstanding the proposal set forth here, that posture ought to continue to be the inclination moving forward. The best policy, where possible, is for ISPs not to be in the job of the gatekeeper: they would ideally

be in the role of passing all packets from sender to receiver, with decisions about what to send and what to receive determined at the end-points. Any departure from such an approach must be taken up only when serious circumstances warrant; where the regulation is handled with a light touch; and where the new burdens placed on the intermediaries are not viewed as an entry point for more intrusive regulatory hooks.

It is essential to acknowledge the Internet has changed since its inception. We use the network far differently than any of its early architects could possibly have imagined. The community of users is now more far-flung than it ever was; users no longer expect to know one another, as the earliest academics and military users did. The Internet's architecture is a victim of its own success as a matter of design. The conventional wisdom that no intelligence should be built into the heart of the network – the so-called end-to-end principle – is still held dear by many technologists, but is no longer the practice in a meaningful sense, as a large number of points of control have been built into the network, often placed there to deal with massive problems like spam.[xxiii] ISPs still enjoy broad immunities – from copyright and defamation claims based on what others do on their networks – in many jurisdictions, but they are increasingly called upon to play a role in protecting and policing the network. There are substantial risks associated with placing such jobs in the hands of ISPs – particularly to civil liberties – and legislation that supports such regimes must be carefully drafted so as to mitigate these risks.

The suggestion in this paper is that countries establish an industry-led regulatory approach that provides a hook for regulators to step in against the worst actors. The proposal is, explicitly, not meant to presage a wholesale shift in the presumption related to the roles of ISPs; nor is it meant to indicate a shift away from adherence to the end-to-end principle as a preferred design matter. ISPs already bear the brunt of the costs of spam. The role of the law and the regulator should not be to overburden ISPs further, especially given the constraints they already face.[xxiv]

The law should function here as a leveling force. The goal of this regulation should be to reduce spam in a manner that establishes a fair and competitive environment for the protection of responsible ISPs that abide the law. As the Internet has developed into a complex network of networks, ISPs are positioned, for good or ill, as key gatekeepers. ISPs that implement responsible, effective anti-spam measures, while preserving the civil liberties of their users in a manner that is consistent with local law, should be rewarded for their good behavior. One means of rewarding those responsible ISPs is for regulators to hold accountable their competitors who are irresponsible. It is this dynamic of a level playing field for responsible ISPs that the proposal in this paper seeks to establish.

ISPs are no stranger to tussles over spam. ISPs from many countries around the world have taken an active role in fighting spam at the source and, on the receiving end, before it gets to their customers' inboxes. These anti-spam measures undertaken by ISPs cover a wide range. Many ISPs participate in industry-wide working groups, such as the Messaging Anti-Abuse Working Group,[xxv] and standard-setting organizations working on relevant technical solutions.[xxvi] Initiatives within the ISPs' operations are often geared toward improving security and decreasing the vulnerability of users and of networks – and, in a functioning market with choices of e-mail providers, these measures can take the form of competitive advantage for the ISPs. For example, Google's Gmail, a free web-based e-mail service, removes hyperlinks from messages that the service believes to be "phishing" attempts.[xxvii] The large United States-based ISP Earthlink requires all e-mail messages to route through its mail servers to reduce the impact of zombie networks and mandates that users' e-mail programs submit passwords to transmit

messages.[xxviii] While these methods can reduce the burden of spam, their effect is minimal if consumers do not also take steps at the "client" level of the network. Users who do not update virus software and operating systems automatically or regularly, or who download programs that contain "malware" and "spyware" that compromise their computer, pose a risk not only to themselves but to other users worldwide, since their personal computers may be used to relay spam to other unsuspecting customers.

The incentives of law-abiding ISPs are well aligned with the interest of the state in the common desire to end spam.[xxix] ISPs bear a large amount of the cost of spam and get nothing in return, so long as those same ISPs are not charging a premium to spammers in exchange for sending spam out on their behalf. ISPs also are relatively close to the problem; a spammer needs an ISP to get access to the network to do their nefarious deeds. While spammers are increasingly sophisticated in their actions to evade those who would track them, in most instances, a concerted effort among cooperating ISPs (and possibly law enforcement officials and end-users) can result in finding the worst offenders. The travel of spam can be traced and mapped at a network level.[xxx] While ISPs are often in very competitive situations where cash-flow is tight, many ISPs do have the financial and human resources to play a key role in the anti-spam fight – and which efforts, at least at the level of collective action, will redound to their own benefit and that of their customers.

Under this proposed approach, the law of a given country would mandate the development of codes of conduct for and by Internet Service Providers (ISPs). The establishment of these codes might be set as a condition of a license, or permission to provide Internet services to citizens. Alternately, this mandate might be implemented through rule-making, via a common set of regulations that applies to ISPs whether licensed or authorized, much as operators are required to provide interconnection, the rules for which are spelled out in interconnection regulations. Such a code of conduct would be developed as part of a light-handed, industry-driven regulatory process. In this scenario, the law would require that regulators grant to ISPs the first opportunity to create a code of conduct outlining appropriate use of its service by its customers (i.e., prohibiting spam, phishing, spoofing, and comparable anti-social behavior on the network), as well as suggestions regarding the best use of spam filters and other technological tools that customers and ISPs themselves can take to fight spam. Under such codes, ISPs would commit themselves to denying service of any kind to spammers, phishers, spoofers and other bad actors who violate these policies. Such codes of conduct would be led by industry and made functionally consistent among all players across the industry, but as part of a process that is grounded in law and provides a role for regulators. The regulator would be empowered to approve the code and to enforce the code if the ISP deviates from its terms in material fashion.

Regulators are better able to do their job under this scenario, as compared to the straight enforcement role against spammers, since the regulators would primarily interact with ISPs. The ISPs are largely running legitimate businesses, are incentivized to help solve the problem (so long as they are not cheating), and are easy to find relative to the spammers, who are often not in the same country and are constantly hiding behind technological smoke and mirrors. The ISPs, in turn, would be responsible to keep tabs on those customers who are engaged in illegal activity and to spurn offers for premium payments to provide spammers with an onramp to the Internet. This paper discusses how such enforceable codes of conduct could be developed such that industry, which best understands technological solutions to the spam problem, takes the lead in drafting the code, while leaving to regulators the job of approving the code and ensuring that ISPs abide by it. This mechanism would empower the regulator to apply a default code of

conduct where ISPs fail to develop one or until an acceptable policy is set forth by the ISP. Such a mechanism would also include the regulator's certification of the code which ISPs could use in their advertisements, to ensure customers that the ISP is taking all available steps to protect its customers, and the network at large, from spam. The system would also involve a reporting mechanism so that victims of spam, phishing, spoofing and the like can report such activity either to the ISP or the regulator for follow-up investigation and action.

Such an enforceable ISP Code of Conduct is not without drawbacks. The hazards associated with this approach, explored in greater depth below, must be carefully mitigated. As an enforcement mechanism, its terms must be narrowly tailored to curb spam and related bad acts; it should not be used as a back-door measure to over-regulate ISPs, either by imposing anti-spam obligations where no technical solution has yet been developed (e.g., currently, many anti-spoofing requirements suffer from such a problem) or by using anti-spam measures as a means to limit legitimate political discourse or other protected speech or to infringe upon the privacy interests of citizens. It is essential that such codes be developed by industry and approved, or at a minimum developed together with industry in a collaborative process, and that the codes are frequently updated to take into account new developments in spamming practices and anti-spam technology.

Under a variant of this formal legal approach, the regulator could formally encourage ISPs to develop their own codes of conduct. Many ISPs are taking this step without any encouragement from regulators, which policies are effectively expressed through Acceptable Use Policies for customers and for ISPs with whom the ISPs enter into peering relationships.[xxxi] Under this voluntary scheme, the regulators may assist the industry in developing these codes of conduct. The regulator might also provide assistance to consumers seeking to determine which ISPs have effective codes of conduct and which do not. Though far less likely to be effective than other measures, it is conceivable that a functioning market could emerge, wherein consumers choose ISPs, where there is competition, in part based upon their reputation in terms of fighting spam.

Finally, regardless of whether ISPs are compelled to establish enforceable codes of conduct, regulators have an important role to play in educating and raising awareness among consumers, businesses, ISPs and cyber café operators both on technical solutions such as spam filters, and warning about fraudulent activities like phishing. This chapter will explore in brief the kinds of information regulators can disseminate as well as suggest means of disseminating such information.

II. An Outline of a Model Law.

A. The Context for a Model Anti-Spam Law.

Representatives of many countries, particularly in developing areas, have sought a model law for combating spam. The topic of a model law has received considerable attention at two international gatherings hosted by the International Telecommunication Union, one devoted to spam in the summer of 2004 and another on cybersecurity more generally in the summer of 2005. This paper is intended to draw upon the many resources developed to date and to press forward in the process of developing such a model anti-spam law. The outline set forth in this paper is offered with the understanding that the process of refining a model law must also be an inclusive, carefully designed one that is carried out over an appropriate period of time.

An earlier paper, "A Comparative Analysis of Spam Law: The Quest for A Model Law" has made the argument that the benefits of a model anti-spam law are several-fold:

- **Clear guidelines** – Senders who want to comply with applicable legal requirements could more easily learn what rules apply and could follow them more cheaply and consistently, since they would not have to attempt the near-impossible task of tailoring messages for recipients in different jurisdictions.

- **Easy adoption** – Legal systems that do not yet have laws governing spam would have a ready-made model to implement, reducing the burdens of drafting, implementation, and coordination.

- **Enhanced enforcement** – Regulators could enforce laws more effectively and easily since their systems would share harmonized definitions of offenses, burdens of proof, and exceptions. Greater harmonization would make broad-based cooperative arrangements more likely to arise.

- **Stronger norms** – Broad international consensus on the meaning of spam, and what constitutes unlawful communication, would strengthen norms that deprecate such conduct.

- **Fewer havens** for spammers – As more regimes adopt the model law, spammers would have fewer locations friendly to unlawful activity where they could establish operations, increasing their costs and reducing the financial incentives to engage in this behavior. In addition, harmonized legal provisions will increase pressure on systems to adopt meaningful regulations rather than loose ones that facilitate a domestic spam hosting industry. (In particular, the ISP code of conduct notion introduced in this paper is designed to address this substantial concern.)

- **Increased sharing of best practices** – Since legal systems would share harmonized provisions, regulators and enforcers could more easily collaborate upon, develop, and share best practices for implementing spam laws.[xxxii]

While even a well-crafted anti-spam law in every relevant jurisdiction will never get the job done alone, common anti-spam legislation can be a useful element of a coordinated anti-spam strategy. A good anti-spam law ought to "distinguish between good actors and bad actors and

mete out punishment accordingly. If each spam message sent carries with it a credible risk of a fine or other punishment to the spammer, then the effective cost of sending spam will correspond with the volume a spammer produces."[xxxiii] The law must be backed by a reasonable expectation that it will be enforced if violated. It is this enforcement mechanism that poses the broadest challenge in the business of anti-spam. That problem is most acute in the developing countries context. An anti-spam law is most likely to be effective in direct proportion to the extent to which it is geared toward being possible to enforce by regulators.[xxxiv]

The process for developing a model anti-spam law ought to be pursued collaboratively and inclusively. After such a process, a full model law would be more substantially built-out and include further annotations and options than that which we provide here in this outline. This attempt is to set in place a draft outline, drawing upon the good work of many actors to date, from which a country might work in developing their own statute or as a basis for a full-blown model law, which would need to be extensively vetted. As with any model law, (or, for instance, a directive of the sort passed by the European Union), the proposal must be flexible enough to be able to be integrated with the general types of law in the jurisdiction. Other laws that should be considered, from an integration standpoint, include anti-fraud legislation, consumer protection legislation, and telecommunications and internet-specific legislation (such as computer fraud and e-commerce laws). A relevant process to consider is that which UNCITRAL undertook in establishing its Model Law on Electronic Commerce (1996).[xxxv] UNCITRAL's E-Commerce model includes a number of relevant sections, elements of which have been adopted in dozens of jurisdictions, but it does not address spam *per se*, which did not exist in anywhere near its current form in 1996. Such a model law development process ought also to consider the broad range of laws on the books today, many of which include variations worth considering that are omitted in this report for space purposes only.[xxxvi]

Most of the existing anti-spam laws are directed at controlling the behavior of spammers. This emphasis is appropriate at a conceptual level, since spammers themselves cause the problem. In light of the fact that the current slate of laws has failed even to curb the *growth* of spam, much less to eradicate the problem, the core function of these laws is subject to examination.[xxxvii] Why have they failed?

There are many reasons that contribute to the failure to date of the current slate of anti-spam laws. Some observers argue that the countries that generate the highest proportional amounts of the world's spam – the United States probably chief among them[xxxviii] – have done too little at home to stop the problem within their own country and beyond, especially in relying upon opt-out rules and then not enforcing them aggressively enough. This blame can be spread much further than the greatest spam-producing nations, though; no country in the world, including those lauded as the most effective in combating spam such as Australia, has made terrific inroads through classic enforcement mechanisms. Another problem is that states have not yet been learning from their mistakes by updating anti-spam laws in light of their now-obvious inadequacy. Others point to the fact that anti-spam laws should be focused not on the spammers themselves, but rather those on whose behalf the spam was sent.[xxxix]

The primary issue with these extant laws is that there is too little emphasis placed on investigation, enforcement powers, and resources to carry out the enforcement in a way that is likely to work against such a distributed problem. The issue is not so much that any one case is so hard to build, mount, and win – most spammers or those who commission them to send the mail can ultimately be found, if enough people cooperate – but rather that each investigation is

so intensive and complex as to result in an unfavorable (to the enforcer and to the public at large) cost-benefit equation. One of the core tenets of the model law described here is that it emphasizes creating a framework for national enforcement, international coordination in terms of enforcement, and distributed enforcement through the ISP code of conduct provisions.[xl]

B. Elements of a Model Spam Law.

This model law, proposed here as an annotated outline, follows roughly the structure of the Australian anti-spam law, which is widely regarded as one of the most well-conceived statutes of its kind in the world.[xli] What follows is an outline of key elements of a model law, a functional description of each segment (not intended to be suitable as the actual legislative language for each jurisdiction, of course), and annotation designed to help the drafter consider important options at each stage of the drafting process. For instance, by way of annotation, we note a number of important issues that a draftsperson would need to take up at the outset of developing an anti-spam statute.

One such threshold issue is whether the law will be an "opt-in" or an "opt-out" statute at its core. In an opt-in statute, the law states that it is illegal to send spam unless a recipient has affirmatively agreed to receive such an electronic message or otherwise indicated her assent (often through a pre-existing business relationship of some description). In an opt-out statute, the law states that it is illegal to send spam if a recipient has told the sender that the recipient does not wish to receive messages from the sender. The effects of such a decision reverberate through the law thereafter. For instance, if the law is grounded in an opt-out system, the language for a requirement to have an unsubscribe function is, at least conceptually, more essential and takes on a different character than if the system is opt-in, which presumes that the receiver initially exercised an affirmative choice before receiving any messages.

We also delve into a series of important definitional issues at the outset of the draft model law. One deficiency of many of the extant spam laws is a lack of clarity at the definitional level and problems that stem from variation among definitions across jurisdictions that might otherwise cooperate to enforce their respective laws.

Draft Model Law

Section 1: Introduction and Definitions. The law ought to clarify that it establishes a scheme for regulating commercial e-mail and other types of commercial electronic messages.

> *Annotation: The introduction section of the law ought to set forth a series of important definitions. While definitions are always important in legal drafting, they take on special significance in the anti-spam setting. On the one hand, the terms must be broad enough to encompass emerging types of ICT-related spam as they inevitably develop as new technologies become popular; on the other, the provisions must be precise enough to be understood by the governed. In addition, given that anti-spam statutes nudge up against important civil liberties, such as speech and personal privacy (more honored in some jurisdictions than in others), definitions may play a pivotal role in whether the statute is*

permissible under a country's constitutional framework and/or sufficiently protective of the rights of citizens.

The following are some of the key terms to be included in the definition section of the Model Law, though by no means a complete list:

- **Address-harvesting software.** The law should define the types of computer applications used for the harvesting of e-mail addressed from the Internet which are banned, or the trafficking in or use of which is banned, (if such a provision is included), under the statute.

  Annotation: An important question for any anti-spam law is whether or not to include a prohibition on the use of or trafficking in the technologies that support spamming, such as address-harvesting software. If included in the model law, the term must be carefully defined so as to avoid banning useful technologies of general applicability that may be used for address-harvesting. Another approach – to some policy advisors, vastly preferable – is not to ban the technology, but rather to bar its use for the prohibited end of gathering e-mail addresses then used in spamming.

- **Authority, or Regulator.** The law should specify the regulator under whose jurisdiction the anti-spam law resides. Countries vary as to the precise placement of this authority, which might be vested in the telecommunications regulator, the consumer protection authority, the trade regulator, or another regulator of commercial activity.

  Annotation: If multiple regulators are charged with enforcing the anti-spam rules, precise division of responsibility should be established, either in the definitions section or, more likely, below under the enforcement-related provisions.

- **Authorization.** The law should clarify what it means for an individual to authorize a sender to send a message.

  Annotation: This definition may take on greater or lesser significance depending on whether the law is designed as opt-in rather than opt-out. Depending upon the nature of the law adopted and the use and definition of the term "Consent," below, this definition might not be necessary.

- **Commercial.** The law must specify with precision what constitutes a message sent for commercial purposes. Commercial messages among senders and recipients who do not have a previous commercial relationship are likely to serve as the core, prohibited type of content.

  Annotation: One key issue facing development of a useful model law is the variation in the treatment of speech rights in different jurisdictions. In Australia and the United States, for instance, legislators and regulators have stayed clear of regulating unsolicited political messages in light of constitutional protections in both places for political speech.

Most anti-spam laws focus not on the content of the message, but rather on the intent of the sender. Spam legislation varies as to whether or not the prohibition is circumscribed so as to apply only to commercial messages, but in any event commercial messages most likely must be carefully delineated at the outset. Intent-based statutes suffer from a well-known set of deficiencies, but in this case, it seems to be the consensus that an intent-based rule is necessary. The counter-argument is that the emphasis on intent rather than content might make the statute less likely to harm the rights of free expression of citizens.

- **Consent (or, Affirmative Consent).** The law should clarify what the recipient had to do to indicate her or his willingness to enter into correspondence with an e-mail sender. For instance, the law might state that the term ''affirmative consent'', when used with respect to a commercial electronic mail message, means that (A) the recipient expressly consented to receive the message, either in response to a clear and conspicuous request for such consent or at the recipient's own initiative; and (B) if the message is from a party other than the party to which the recipient communicated such consent, the recipient was given clear and conspicuous notice at the time the consent was communicated that the recipient's electronic mail address could be transferred to such other party for the purpose of initiating commercial electronic mail messages.

  Annotation: As noted above, this definition should be coordinated with the definition of the term "authorization," as needed.

- **Electronic message.** The law must specify, for the purposes of this Act, what constitutes an electronic message. In the Australian example, an electronic message is a message sent: (a) using: (i) an Internet carriage service [the term to be amended depending on local descriptions of ISPs, ESPs, and the like]; or (ii) any other listed carriage service; and (b) to an electronic address in connection with: (i) an e-mail account; or (ii) an instant messaging account; or (iii) a telephone account; or (iv) a similar account.

  Annotation: An important area to consider is what applications are covered by the anti-spam statute. The best anti-spam laws will be general enough to cover information and communications technology-based unsolicited messaging in formats that have yet to be devised as well as the range of formats that exist today. Short Messaging Service (SMS) text messages on cellular phones, spam over the instant messaging protocol ("spim"), web blogs (especially in the comments fields), and Really Simple Syndication (RSS) are important current variants of traditional e-mail spam that drafters may wish to keep in mind.

- **Evidential (or evidentiary) burden (or, burden of proof).** The law should define carefully, in relation to a matter, which party bears the burden of adducing or pointing to evidence that suggests a reasonable possibility that the matter exists or does not exist.

  Annotation: The relative importance of this provision, of course, will depend upon the nature of the judicial process in a given jurisdiction. It is included here because one of the key problems that enforcement authorities have faced is a high burden of proof

placed upon the prosecution in instances where they must show conclusively that a user did not opt-in to communications with the sender. Virtually no individual can prove the negative that they never entered into a commercial relationship, or once hit "OK" in a click-through contract, that permitted a sender to contact them; to place the burden on the regulator to prove this negative is to hamstring her or him in the enforcement process.

- **Internet service provider** (or Internet carriage service; Internet content provider; E-mail service provider; Telecommunications service; or the like depending upon jurisdiction). The law should define what types of service is covered by the statute. The essential part of the definition is that the covered party is one that provides a connection between an end-user and the Internet for a fee.

  Annotation: In many jurisdictions, a wide range of definitions for ISPs are established across various Internet-related laws, so special care should be taken to tie definitions across statutes for clarity's sake. United States law, for instance, has more than 40 potential definitions for terms that resemble "Internet service provider."[xlii] *The integration of this definition with the rest of the country's law, to limit ambiguity, is important in particular for this model law, which contemplates setting an affirmative requirement for ISPs to develop an enforceable code of conduct.*

- **Send.** The law should clarify that the definition of "send" includes attempts to send.

[*End of (partial) definition section.*]

Section 2: It is unlawful to send unsolicited commercial electronic messages.

Annotation: The scope of what type of message is unlawful to send, combined with the definition of the terms of what is banned, is a crucial element of any spam law. States vary widely in terms of whether messages outside of the core "unsolicited commercial e-mail" is included under the ambit of the law. For instance, non-commercial bulk e-mail is included in the definition of "spam" in some anti-spam legislation and not in others. This is also the juncture where each country must decide whether to join the opt-in or opt-out camps. Virtually all anti-spam laws focus upon the act of sending (or attempting to send) as the core, operative offense. An additional prohibition for this section might be to hone in on the act of paying someone to send unsolicited commercial electronic messages on one's behalf. Some states also bar the sending of unsolicited charitable and issue-oriented (political) messages, but that step is dangerous and not advocated here, given the importance of political speech to well-functioning government systems.

Section 3: Commercial electronic messages must include accurate sender information.

Commercial electronic messages must include information about the individual (or organization) who (or that) authorized the sending of the message.

Annotation: The law might also require that commercial email be identified as an advertisement, with [ADV] or the like in the header, and include the sender's valid physical postal address. Possible terms include stating: "Commercial electronic

messages must contain clear and conspicuous notice that the message is an advertisement or solicitation and that the recipient can opt out of receiving more commercial email from you. It also must include the sender's valid physical postal address." Some activists have also called for the requirement that senders label sexually-explicit messages with [SEXUALLY EXPLICIT] in the subject line. The requirement of labeling, such as the added [ADV] or [SEXUALLY EXPLICIT] in the subject line, is hotly contested by e-mail marketers, who fear that all such messages, even if legitimate commercial offers in which individuals are interested, will be filtered into trash folders in e-mail clients and by ISPs.

Section 4: It is unlawful to include false information in any commercial electronic messages.

Commercial electronic messages must not include false information. An email's "From," "To," and routing information – including the originating domain name and email address – must be accurate and identify the person who initiated the email. The subject line cannot mislead the recipient about the contents or subject matter of the message.

Annotation: Most experts contend that an anti-spam law ought to contain such a ban on inclusion of false information as a supplement to other provisions, such as the outright bar against sending an unsolicited message. This fourth provision on its own, without the additional hooks, is critiqued as de facto permitting spam that is unwanted but otherwise accurate. Much of the criticism leveled against the US CAN-SPAM Act of 2003 has followed such a line of argument.

Section 5: It is unlawful to send a commercial electronic message without a simple means for recipients to indicate that the recipients do not wish to receive any further commercial electronic messages from the sender.

Commercial electronic messages must contain a functional unsubscribe facility. If a recipient exercises his or her right to indicate that he or she does not wish to receive future messages from the sender, the sender must honor those requests. [Or, if the regime is an opt-in regime, such a provision would ensure that a recipient who had previously opted-in could opt-out at any time, after which time the recipient would be treated for legal purposes as not having opted in, from that the time of unsubscription forward.]

Annotation: In the United States, for instance, a sender must provide a return email address or another Internet-based response mechanism that allows a recipient to ask the sender not to send future email messages to that email address. The sender must honor the requests. Any opt-out mechanism a sender includes must be able to process opt-out requests for at least 30 days after commercial email is sent. When a sender receives an opt-out request, the law gives 10 business days to stop sending email to the requestor's email address. A sender may not help another entity send email to that address, or have another entity send email on your behalf to that address. It is illegal for a sender to sell or transfer the email addresses of people who choose not to receive that sender's email, even in the form of a mailing list, unless a sender transfers the addresses so another

entity can comply with the law. These provisions, while sensible, are believed to have a very low rate of compliance. Most critics also believe that unsubscribe responses by recipients are frequently used to add to spamming lists, since the spammers then know that the address reaches a real recipient.

Section 6: The use of and trafficking in address-harvesting software and the resulting lists of electronic mail addresses are prohibited.

Address-harvesting software must not be supplied, acquired, trafficked in, or used. An electronic address list produced using address-harvesting software must not be supplied, acquired, trafficked in, or used.

Annotation: There is a wise presumption generally against banning technologies that may be general purpose in nature. Any provision of this sort ought to bear in mind, and exempt, the makers of general purpose technologies (for instance, a spreadsheet or software enabling a user to write a simple program that could scrape information from the web) that might be used by spammers to harvest e-mail addresses. The law might also include a prohibition against hacking into databases of e-mail addresses, though in many jurisdictions, such acts would be covered under statutes related to computer crimes, the common law of larceny and/or trespass, or equivalent laws.

Section 7: Remedies include civil penalties, injunctions, and criminal penalties.

The main remedies for breaches of this Act are civil penalties and injunctions. Criminal penalties are also sometimes sought, including imprisonment, when false representation, use of another's computer to perpetrate a fraud, or the like is involved.[xliii]

Annotation: The law might also include a provision making it a criminal offense for an ISP knowingly to accept premium payments from spammers who use the ISP's network to send their spam. Similarly, the law might include a provision that makes the knowing hiring of a spammer to send out unsolicited commercial e-mail a criminal offense.

Section 8: Causes of Action.

The law ought to establish a cause of action for regulators against someone who pays a spammer to spam for them (i.e., the owner of a website to whom a spammer is paid to direct traffic, or the party seeking to drive up the value of a certain equity offering, e.g.).[xliv] The law might also include additional causes of action, such as those that enable an ISP, enforcement officers in lower jurisdictions, and individuals or others who are harmed to initiate a case.

Section 9: International Cooperation.

The law ought to create a mechanism for information-sharing internationally and, possibly, formal cross-border enforcement support. These rules would be geared toward the facilitation of cross-border enforcement, simplifying the process for exchange of information among

regulators, and encouraging exploration of Memoranda of Understanding and similar means of cross-border cooperation.

> *Annotation: Much of the emphasis of far-sighted regulators in recent years has been on improving cross-border enforcement efforts. The US FTC has been encouraging the US Congress to pass a law to make such cooperation more likely to succeed. Consider also the work of the International Consumer Protection and Enforcement Network, which joins dozens of countries to conduct "sweep days" to rid the Internet of scams.*[xlv]

Section 10: Jurisdiction.

An effective anti-spam law might include provisions designed to assist enforcers by resolving jurisdictional ambiguities.

> *Annotation: Such a provision could simply clarify what it means for a message to originate or be received within that country and how the regulator will treat such situations. On a more elaborate level, in the United States, the state of Washington's anti-spam law established a database that includes many of the e-mail addresses in that jurisdiction for the purposes of protecting the state's residents.*[xlvi] *Such an approach bears with it the security concern and hazard that a list of that nature held in one place would be an attractive target for hackers. This concern is mitigated by the fact that spammers apparently do not have much of a problem coming across large swaths of e-mail addresses through other means.*

Section 11: Enforceable Codes of Conduct by ISPs.

An effective anti-spam law might include sections related to the development and enforcement by regulatory authorities of industry-derived and implemented Codes of Conduct to be applied to ISPs.[xlvii] [Include on this page when printed a text box with the Australian code of conduct provisions.] Such provisions might include:

a. An introduction, explaining the intention to establish such codes of conduct.

b. A provision granting the regulator, or regulators clearly delineated, to require all ISPs to develop a code of conduct specific to that jurisdiction.

c. A description of the process, involving as many stakeholders as practical, to be involved in the development of codes of conduct, including those who could press the interests of members of the public, consumers, and industry.

d. A provision establishing a registration process for codes of conduct.

e. A provision enabling consumers to access registered codes of conduct.

f. A provision enabling the regulator to develop a code of conduct in the event that industry cannot agree or otherwise fails to enact a code of conduct.

g. A provision enabling the regulator to reject a proposed code of conduct in the event that it lacks appropriate community safeguards.

h. A description of the process for the regulator to issue a warning to an ISP for apparent breach of the code prior to taking an enforcement action.

i. A provision granting power to the regulator to enforce the code in the event of breach by the ISP.

Annotation: A similar structure is set forth in Part 6 of Australia's Telecommunications Act of 1997 covering industry codes of conduct. There are a number of issues to be considered, many of which are set forth in the section that follows. The law would need to establish a timeline for compliance from the enactment of the law and provide for periodic updating of the code. One question is whether, where an industry association exists for all or part of the ISP industry within a given jurisdiction, that industry association ought to be tasked with leading development of the code of conduct. If such an association establishes a code of conduct that is acceptable to the regulator, must all ISPs within the jurisdiction adopt an identical code? The enabling provisions for the code might ensure that an ISP may opt out of a code developed in a group process, and register that separate code with the regulator, provided the ISP's self-developed code is sufficiently protective of the public interest as determined by the regulator.

III. Codes of Conduct for ISPs, Network Operators, and Other ICT Data Carriers.

This paper suggests that countries drafting an anti-spam law, especially developing countries, consider establishing enforceable codes of conduct for ISPs and other entities that might transmit spam. The primary goal of such a set of provisions is to ensure that ISPs that provide a route to the Internet – the source ISP – are taking adequate steps to keep spammers off the network. The net effect of such a set of regulations ought to be to level the playing field for those ISPs that are actively seeking to rid the network of spam, rather than seeking to profit from sourcing it. While there are many risks attendant with regulating ISPs more extensively than they have been in the past, a carefully balanced set of provisions will redound to the benefit not just of customers, but of all well-intentioned ISPs as well.[xlviii]

In virtually all instances, industry is better placed than most regulators to know what technical solutions to spam exist and are likely in the best position to ensure that such technical solutions are implemented.[xlix] Regulators have a role to play to ensure that industry does all that it can to implement such technical and policy solutions and to share best-practices where industry members do not have visibility into the effective practices of others.

The use of industry codes of conduct is a promising mechanism that has been under-utilized in the anti-spam fight. A similar strategy has been used for a variety of other issues, such as interconnection, number portability, and other technical coordination issues in telecommunications. If combating spam is not in the remit of the telecom regulator, a similar mechanism could be established for consumer protection authorities, data protection authorities or other similar bodies. For the purposes of this chapter, the code of conduct has been included in a model anti-spam law, but such a set of provisions could easily fit within other sections of a country's legislation, such as the telecommunications laws and regulations generally. The code of conduct does rely, however, upon core elements of an anti-spam statute.

A. Procedural Steps Toward an Enforceable Code of Conduct.

Industry codes of conduct should be developed in the spirit of minimal regulation of the Internet and as a measure of private and public sector cooperation to address the growing problem of spam. The development of such codes of conduct would include several key steps:

- The relevant industry member or members are granted the first chance to develop their own code of conduct, based upon the stated goals of the regulations. The process by which a draft code is established should be set forth in the regulations so as to ensure broad and open participation by key stakeholders.

- Where appropriate, the regulator can help in code development, by way of sharing best practices. Regulators may be better able to tap into international resources such as the OECD's Spam Toolkit, which is under development (a draft is accessible at http://www.oecd.org/document/24/0,2340,en_2649_22555297_34804568_1_1_1_1,00.html).

- The relevant industry member or members present(s) the code to the regulator for its approval.

- A new body, or an existing regulator with relevant expertise, takes responsibility for the administration and registration of the code.

- If industry fails to develop a code, or if the code is not deemed acceptable, the regulator has the power to develop a code for industry or revise the code to ensure sufficient anti-spam measures are being taken by ISPs, network operators and other potential spam carriers.

- The industry members are expected to enforce the code against their customers and those with whom they peer. The enforcement is meant to prohibit the worst acts of spamming, not to encourage an ISP to inquire into the nature of any more messages sent through their networks than they ordinarily do. The expectation is that ISPs would only need to take reasonable measures, such as investigation when the ISP receives an unusually large numbers of complaints against a single customer or when the regulator passes along such complaints.

- The regulator or administrator provides a mechanism for handling complaints from end-users against an ISP for failure to live up the code. Large volumes of complaints against a single ISP from multiple sources should be the primary guide to enforcement of the code.

- If industry members fail to enforce the code, the regulator is empowered to take action against non-compliant ISPs. Possible sanctions include fines levied against the ISP, the introduction of harsher licensing requirements, or lawsuit.

  Annotation: One issue to consider is which parties would have a right of action to sue a non-responsive ISP. For instance, consumers who have been damaged by spam or phishing, but who have not been able to convince the regulator to bring an action against an ISP, might gain recourse to go to court to sue the ISP directly for violation of its code of conduct. Another way to achieve the same end might be to require ISPs to include adherence to their code of conduct as a pledge made by the ISP to consumers under their usage contracts, enabling consumers to sue not under the anti-spam law but as a straight breach of contract matter in those jurisdictions with such a cause of action.

- The code might also allow for the creation of a "certification" or "accreditation" system, whereby ISPs that have agreed to comply with the code can advertise to their customers that they are a signatory to such a code. Such an accreditation mechanism might function as other trustmark organizations, such as TrustE, do in a business ecosystem, helping consumers with limited time to make reasonable decisions about which service to choose.[1] Such an accreditation process would be most important in the event that the code of conduct process were encouraged, but not mandated, by the regulator.[li]

- The code should also include a mandatory review or sunset clause provision to ensure that the regulation remains appropriate in a fast-changing technological and legal environment, and to ensure periodic public review.

These procedural steps ought to be designed with a view toward ensuring that the resulting codes of conduct are optimally designed to address the spam problem as it continues to morph, while limiting the negative externalities to which such provisions might give rise.

B. Elements of a Model Industry Code of Conduct.

Like a model law, an industry code of conduct ought to be developed through an inclusive, carefully orchestrated process designed to elicit the best thinking from a range of experts and concerned stakeholders.[lii] The code should set forth the responsibilities of ISPs and other carriers with regard to spam in a manner that is sensitive to local concerns, yet takes into account the cross-border nature of the problem. Key elements of a model industry code of conduct might include:

- A series of common definitions that tie directly to the definitions set forth in the relevant law.

- A set of suggested procedures to be followed by ISPs in dealing with obvious spam that comes into the ISP's sub-network (including procedures relating to the provision or use of regularly updated software for filtering spam).

- A commitment not to provide services to those who send unsolicited commercial email in bulk and to terminate those clients when complaints, and subsequent investigation, reveals that the client has been spamming through the ISP's network. This commitment also includes agreement to refuse any payment, or premium payment, offered by a known spammer for any services.

- A commitment to giving subscribers to the ISP information about the availability, use and appropriate application of software for filtering spam at the client level. A similar commitment to giving customers plain-language advice on how to prevent their computers from being infected by worms, trojans, or other malware that turn computers into spam "zombies," and provide the appropriate tools and assistance.

- A commitment to taking action to assist in the development and evaluation of software for filtering spam that gives the user maximum levels of control over their decisions of what to accept and to reject.

- A series of suggested best practices, not required by the law but recommended by the code, that may be taken as appropriate in order to minimize or prevent the sending or delivery of spam. At present, such suggested best practices might include some of those set forth in the London Action Plan.[liii] The London Action Plan is the result of a meeting in late 2004 of "government and public agencies from 27 countries responsible for enforcing laws concerning spam" who "met in London to discuss international spam enforcement cooperation. At this meeting, a broad range of spam enforcement agencies, including data protection agencies, telecommunications agencies and consumer protection agencies, met to discuss international spam enforcement cooperation. Several private sector representatives also collaborated in parts of the meeting." Recommendations derived from these expert gatherings include:

    - The optimal configuration of servers and other network devices so as to minimize or prevent the sending or delivery of spam;
    - A commitment to taking meaningful zombie-prevention measures;[liv] and,

- A statement of principles relating to entry into peering arrangements only with those ISPs which also abide in full the code of conduct, to establish a virtuous circle.

The draft provisions of a code of conduct will no doubt change rapidly as the nature of the problem changes. Today, as much as 50 per cent of all spam is sent through "zombie" computers, which suggests that emphasis on helping users to avoid their computers becoming zombies ought to be a high priority. Once this loophole is closed to spammers, the way through the network for unwanted e-mail is certain to change, potentially giving rise to the need to amend the code of conduct to head off other problems. The proposed law ought to be flexible enough to accommodate such certain changes in the technological landscape.

C. Hazards Associated with Enforceable Codes of Conduct.

The adoption of a statute that establishes a regime of enforceable codes of conduct for ISPs is not without hazards. A well-designed scheme should be able to mitigate these hazards, but they are worth considering at the outset.

- Industry Codes of Conduct should be geared toward ensuring that ISPs have the proper incentives to be refusing service to and shutting down outrageous spammers, not to over-regulate ISPs or to encouraging ISPs to block more messages or listen in to more conversations that their users are having. The use of such codes should be strictly limited to requiring ISPs to shut down spammers, and not used for other objectives, such as requiring ISPs to shut down those who use email to send what the government considers as unpalatable political messages, nor for the purpose of surveillance of a country's citizens. This hazard points back to the importance of definitions in the introduction of a model anti-spam law that clarify that only electronic messages of a commercial nature are not to be sent without the appropriate level of permission (contingent upon whether the regime operates on an opt-in or opt-out basis). Overall, the risk of such an approach is that ISPs become more inclined to look into the nature of messages sent across their network. A properly crafted law of this sort should not have this effect, if regulators are certain to focus on the worst, most obvious cases of spamming, rather than pressuring ISPs to shut down legitimate e-mailers for fear of regulatory backlash.

- Enforceable codes of conduct have a key dependency on a well-drafted, basic anti-spam law or provisions in other laws that prohibit the worst acts of spamming. Without such an underlying statute and the threat of direct enforcement against the spammer by a regulator, the ISP, or another affected party, the code approach is less likely to be successful. As referenced above, the provisions that establish a code of conduct might sensibly be placed within telecommunications regulations or otherwise apart from the spam statute, so long as the regulator, and potentially others, has the ability to take direct action against a spammer.

- The political realities in terms of adopting and enforcing such a scheme are likely to be complex in many jurisdictions where ISPs have previously enjoyed broad immunity or where the ISP is a monopoly, state-owned telecommunications provider that actually or prospectively generate important revenues for the government.

- There are costs associated with any new administrative mechanism, even one as simple as the code development, registration, and updating process, which ought to be factored into a country's cost-benefit analysis when considering adopting such a regime.

- There are a variety of downsides related to placing such a large bet on putting ISPs in the role of lead players in the fight against spam. As noted above, adding intelligence to the middle of the network, and encouraging gatekeepers to use this intelligence, is sub-optimal from a network design perspective. Like regulators in developing countries, ISPs may themselves face resource constraints to enforce their code. ISPs may or may not consider themselves properly incentivized to enforce the code (i.e., they may have trouble balancing a desire to attract and retain bad-acting but paying customers v. the cost of transmitting the spam through their network + the regulatory risk/cost of so doing + any loss of other revenues or attendant costs associated with harboring spammers). ISPs may over-enforce the provisions of their own code, resulting in messages not getting delivered to recipients – a far worse outcome, many argue, to dealing with even a deluge of spam. ISPs may also not be as sensitive to the rights of free expression of their users as states are, especially as most speech protections do not extend to non-state action, as in the case of a private actor blocking otherwise protected speech. ISPs would likely pass costs along to end-users, perpetuating the already-vicious cycle of spammers making the rest of the Internet's users pay for their bad acts. In a developing country context, high Internet access costs are already a major barrier to widespread ICT adoption. Such concerns, however, should be seen in the context of the spam problem itself, which is adding to the cost of Internet access and is helping criminals to perpetrate fraud and disseminate destructive code, each of which are bad not only for consumers but also for the ISPs themselves.

Any legal and regulatory approach of this sort should be drafted while bearing in mind and seeking to mitigate these drawbacks. On balance, however, many jurisdictions will likely find enforceable codes of conduct to be a sound policy choice, which effectively distributes part of the enforcement burden to those closest to the source of the spam problem – the ISPs and the end-users.

IV. The Role of the Regulator in Education and Awareness Raising.

The optimal solution to spam would involve no new law whatsoever. If consumers and businesses could take spam-fighting into their own hands, or if it became no longer economically rational to send spam, the problem would be solved at the lowest cost and at the quickest rate. Regulators could establish an enforcement backstop against the worst offenders who perpetrate the occasional fraud, rather than being thrust into an active enforcement role on the front lines of the anti-spam battle. The brunt of the anti-spam enforcement work would be carried out at the further edges of the network in the most distributed manner possible, by those who pay the true costs of spamming – the end users – while regulators focused their enforcement resources on the largest, most complex cases.

Regulators could play a very important role to play in educating consumers, businesses and ISPs about the dangers of spam and the steps they can take to protect themselves against spam and its attendant problems.[lv] The London Action Plan includes some suggestions for best practices for regulators. Specific ideas include:

- Regulators should consider developing a communications plan relating to consumer and ISP education, such as posting information on their websites and developing print materials for distribution to cyber-café owners, consumers, other businesses and ISPs.

- Regulators should provide a simple means for consumers to make complaints about spam, which, in the aggregate form, in turn will be useful both to ISPs and regulators in stopping spammers.

- Regulators should consider creating a "Combatting Spam" section on their websites that would provide information for consumers, businesses, and ISPs about the best anti-spam practices at any given time. Practical advice regarding spam filters, warnings about phishing attempts and spam that carries viruses, information about recent scams carried out over e-mail, and the like would help to empower end-users to participate in the anti-spam campaign. Examples of web sites in use today include:

  Industry Canada's page on Recommended Best Practices for Internet Service Providers and Other Network Operators:
  http://e-com.ic.gc.ca/epic/internet/inecic-ceac.nsf/en/gv00329e.html

  Recommendations of the Commission nationale de l'informatique and des libertés in France (CNIL Republique Francaise):
  http://www.cnil.fr/index.php?id=1539

  Guidance provided by the Korea Spam Response Center, which "KISA (Korea Information Security Agency), which is an affiliated agency of the Ministry of Information and Communication, on January 24, 2003, to receive and handle civil appeals relating spam issues and to carry out anti-spam activities."
  http://www.spamcop.or.kr/eng/m_3_2.html

  The US FTC's Education Pages related to Spam:
  http://www.ftc.gov/bcp/conline/pubs/buspubs/secureyourserver.htm
  http://www.ftc.gov/bcp/conline/edcams/spam/secureyourserver/index.htm

- Regulators should also consider their ability to play a central role in coordinating the sharing of best practices among ISPs, especially in contexts where political will or resources do not exist for the regulator to achieve an enforcement role. The regulator can also help educate ISPs about some of the relatively simple technical measures. Specific measures include the latest information related to the blocking of open relays,[lvi] focus on "botnets,"[lvii] and slowdowns of traffic on port 25 that might make an enormous difference, particularly in the developing countries context.

Consumer and ISP education is a necessary component of spam-fighting strategies, but efforts of this sort has had little effectiveness to date. The limited effectiveness of these measures, however, is not due to their lack of promise, but rather the limited vigor with which they have been pursued and the challenge of communicating highly technical information to a lay audience. Like the other modes of regulation, consumer and ISP education cannot stand alone, without effective technological and regulatory measures to combat spam, but substantially greater efforts in this area by regulators are warranted and would pay large dividends. But regulators should

not lose sight of the fact that end-users, as well as ISPs, are best positioned to make a difference on the front lines of the anti-spam battle.

V. Conclusion.

Despite the challenges that are bound to lie ahead, regulators ought to encourage the adoption of an anti-spam law that is as consistent as possible with that of other states. Such an anti-spam law might involve creation of an enforceable code of conduct for ISPs, which will place the responsibility closer to where the technical expertise lies. The problem with anti-spam laws to date is that they have failed to create an enforceable regime and have failed to bridge the divide between the state and the technologists who are closest to the ways to solve the problem. An enforceable code of conduct for ISPs, while imperfect as a remedy, would help to mitigate these shortcomings of most previously-enacted anti-spam laws.

Any model anti-spam law, or specific regulatory recommendation, must be taken in the context, however, that the effort to fight spam is not going to be won by adoption of any single strategy. The only way to be successful will be to ensure broad international cooperation based on a range of shared strategies, including legal and regulatory mechanisms, technical improvements, market forces, and consumer-oriented strategies. The development of ISP codes of conduct and their enforcement by regulators can immediately contribute in terms of stemming the tide of spam and materially reducing costs to ISPs and consumers.

---

[i] Despite passage of many dozens of anti-spam statutes in jurisdictions across the globe, the problem has continued to worsen. *See, e.g.*, David E. Sorkin, Spam Legislation in the United States, The John Marshall Journal of Computer and Information Law, Volume XXII, Number 1, at 4 (2003) ("…it is generally agreed that legislation has failed to solve the spam problem.") *See also*, Matthew Prince, "How to Craft an Effective Anti-Spam Law," WSIS Thematic Meeting on Countering Spam, July 2004, ITU Discussion Paper, at 10, at http://www.itu.int/osg/spu/spam/contributions/Background%20Paper_How%20to%20craft%20and%20effective%20anti-spam%20law.pdf ("Few people would dispute that around the world the first generation of anti-spam laws has been an unqualified failure.").

[ii] Business Software Alliance, *1 in 5 British Consumers Buy Software from Spam*, Dec. 9, 2004, *at* http://www.bsa.org/uk/press/newsreleases/online-shopping-tips.cfm.

[iii] http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=108_cong_public_laws&docid=f:publ187.108.pdf

[iv] *See* Matthew Prince, "How to Craft an Effective Anti-Spam Law," *supra* note 1, at 3.

[v] For the most comprehensive resource on the world's anti-spam laws, *see* Christina Bueti, "ITU's Survey on Anti-Spam Legislation Worldwide," July, 2005, at http://www.itu.int/osg/spu/cybersecurity/docs/Background_Paper_ITU_Bueti_Survey.pdf.

[vi] For instance, e-mail security provider IronPort Systems asserts that 72% percent of e-mail sent is spam. *See* http://www.ironport.com/company/pp_sci-tech_today_08-10-2005.html.

[vii] AOL claims that spam is down 85% from two years ago, based upon consumer complaint information. However, such a claim does not account for the effectiveness that their filters may have achieved on behalf of customers, nor the changing perceptions of consumer about how much spam is acceptable. The same article that reported AOL's claim of less spam concludes, "But statistics show that the amount of spam is still huge – even worse than it was when the federal act [the CAN-SPAM Act of 2003] was introduced two years ago." *See* http://www.crmbuyer.com/story/45413.html. *See also* http://www.washingtonpost.com/wp-dyn/articles/A30433-2004Dec27.html. There is a dearth of reliable industry-wide data, which is not surprising in light of the distributed nature of the problem and the competition between ISPs to provide the best anti-spam services to consumers.

[viii] For a review of some of the many recent spam statistics, *see* Bueti, "ITU's Survey on Anti-Spam Legislation Worldwide," *supra* note 5; see Michael Geist, "Untouchable: A Canadian Perspective on the Anti-Spam Battle," June, 2004, at 2, at http://www.michaelgeist.ca/geistspam.pdf; *see also*, Derek Bambauer, John Palfrey, and David Abrams, "A Comparative Analysis of Spam Laws: the Quest for Model Law," June 2005, at 7 – 8, at http://www.itu.int/osg/spu/cybersecurity/docs/Background_Paper_Comparative_Analysis_of_Spam_Laws.pdf.

[ix] *See* Chairman's Report, ITU WSIS Thematic Meeting on Cybersecurity, June – July, 2005, p. 2, point 12, at http://www.itu.int/osg/spu/cybersecurity/chairmansreport.pdf (citing a speech by Spamhaus CEO Steve Linford).

[x] http://news.bbc.co.uk/2/hi/business/3426367.stm.
[xi] The AOL Legal Department posts Decisions and Litigation to their web site at http://legal.web.aol.com/decisions/dljunk/. *See also* http://www.theregister.co.uk/2005/08/10/aol_spam_sweepstake/ (regarding the AOL gold bars raffle, in which they planned to give away the assets seized from a major spammer).
[xii] *See* http://abcnews.go.com/Technology/PCWorld/story?id=1029922.
[xiii] *See* David R. Johnson, Susan P. Crawford, and John G. Palfrey, Jr., *The Accountable Net: Peer Production of Internet Governance*, 9 VA. J. L. & TECH. 9 (2004)
[xiv] BBC, *supra* note 10.
[xv] The four modes of Internet regulation were popularized in Lawrence Lessig's ground-breaking book, *Code and Other Laws of Cyberspace*, in 1999 (New York: Basic Books).
[xvi] *See* http://www.itu.int/osg/spu/spam/background.html and, in particular, the Chairman's Report, at http://www.itu.int/osg/spu/spam/chairman-report.pdf.
[xvii] Geist, "Untouchable," *supra* note 8, at 5.
[xviii] *Ibid.*, point 24 at 4.
[xix] It should be noted that even the United States Federal Trade Commission, which is a relatively well-funded regulatory body, had only brought "over 70 cases" as of July, 2005. In light of the billions of spam messages per day, the notion that such an enforcement effort is unlikely to have much effect undoubtedly is apparent to many governments choosing whether or not to devote resources to fighting spam locally. *Ibid.*, point 19, at 3.
[xx] *See* Suresh Ramasubramanian, "OECD Task Force on Spam Report: Spam Issues in Developing Countries," May, 2005, at http://www.oecd.org/dataoecd/5/47/34935342.pdf.
[xxi] This chapter uses the term "regulators" in the broad sense to include any governmental entity that has been given the mandate to combat spam. Thus, the term "regulators" for this chapter may mean national telecommunications or ICT regulatory authorities, consumer protection authorities or data protection administrations.
[xxii] *See* http://www.itu.int/ITU-D/treg/related-links/links-docs/Spam.html for a list of voluntary and enforceable ISP codes of conduct.
[xxiii] *See generally* Jonathan Zittrain, "Internet Points of Control," 43 Boston College Law Review 653 (2003). *See also*, J.H. Saltzer, D.P. Reed, and D.D. Clark, "The End-to-End Argument in Systems Design," at http://www.reed.com/Papers/EndtoEnd.html and "The End of the End-to-End Argument" at http://www.reed.com/dprframeweb/dprframe.asp?section=paper&fn=endofendtoend.html ("But in many areas of the Internet, new chokepoints are being deployed so that anything new not explicitly permitted in advance is systematically blocked.")
[xxiv] *See* John Spence, "Pennsylvania and Pornography: CDT v. Pappert Offers a New Approach to Criminal Liability Online," 23 J. Marshall J. Computer & Info. L. 411 (Winter, 2005) (a good general discussion of the role of ISPs in the network and the difficulties they face).
[xxv] http://www.maawg.org/about/roster/
[xxvi] Many technical working groups have focused on anti-spam-related standards, technologies, and best practices. The IETF, ISOC, and other groups have supported efforts that have involved representatives of ISPS, including the now-scuttled MARID Project (*see* http://www.internetnews.com/bus-news/article.php/3407431), which was preceded by the Anti-Spam Research Group (at http://asrg.sp.am/).
[xxvii] *See* Renai LeMay, *Gmail Tries Out Antiphishing Tools*, CNET NEWS.COM, Apr. 4, 2005, *at* http://news.com.com/Gmail+tries+out+antiphishing+tools/2100-1029_3-5653794.html.
[xxviii] *See* Anick Jesdanun, *Battle Against Spam Shifts to Containment*, ASSOCIATED PRESS, Apr. 15, 2005, *at* http://finance.lycos.com/qc/news/story.aspx?story=48398343.
[xxix] Consider the remarks of Randall Boe, executive vice president of AOL, when he said that "Spam has become the single largest customer problem on the Internet." (Quoted in Thomas Claburn, "Four Big ISPs Sue Hundreds of Spammers," 10 March 2004, Information Week, at http://www.informationweek.com/story/showArticle.jhtml?articleID=18311680.)
[xxx] As one illustration of the fact that spam can be traced, *see* http://www.channelregister.co.uk/2005/09/20/spam_map/.
[xxxi] Consider, for instance, that MAAWG is already promoting industry-wide codes of conduct. *See* http://www.maawg.org/about/.
[xxxii] Bambauer, Palfrey, and Abrams, "A Comparative Analysis of Spam Laws: the Quest for Model Law," *supra* note 8, at 11.
[xxxiii] Prince, "How to Craft an Effective Anti-Spam Law," *supra* note 1, at 4.

[xxxiv] *Ibid.*, at 6. Mr. Prince argues: "The most effective anti-spam laws are action laws that focus on the problems prosecutors face and work to resolve them. If we want anti-spam laws to be effective, our job must be to identify the costs faced by prosecutors and craft laws to reduce those costs."
[xxxv] Accessible online at http://www.uncitral.org/pdf/english/texts/electcom/ml-ec-e.pdf.
[xxxvi] *See* http://www.itu.int/osg/spu/spam/ for a catalog of existing anti-spam laws on the books in jurisdictions around the world.
[xxxvii] Many analysts predicted the failure of these laws at the time they were passed. For one example of a United States-based consultancy, consider Gartner's report, Maurene Caplan Grey, Lydia Leong, Arabella Hallawell, Ant Allan, and Adam Sarner, "Spam Will Likely Worsen Despite US Law," 3 December 2003, at http://www.gartner.com/resources/118700/118762/118762.pdf.
[xxxviii] *See* BBC News, "US Still Leads Global Spam List," 7 April 2005, at http://news.bbc.co.uk/1/hi/technology/4420161.stm (citing a study by security firm Sophos that the US is responsible for sourcing 35% of the world's spam).
[xxxix] *See* the FAQ page for the Coalition Against Unsolicited Commercial Email, at http://www.cauce.org/about/faq.shtml#offshore.
[xl] One interesting, as-yet-theoretical variant to the state-focused enforcement mechanism is the "bounty hunter" system proposed by Prof. Lawrence Lessig of Stanford Law School. Prof. Lessig has "bet [his] job" on the notion that such a distributed system, established by law but pushing out enforcement authority to netizens, would work if enacted. *See* http://www.lessig.org/blog/archives/000787.shtml.
[xli] The Australian law, which took effect in 2003, can be found online (in an unofficial version) at http://scaleplus.law.gov.au/html/pasteact/3/3628/0/PA000260.htm
[xlii] For example, the text of the Communications Decency Act Section 230 in the United States provides immunity to the providers of "interactive computer services" for the content published on their network. These providers are defined as follows: "The term `interactive computer service' means any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet and such systems operated or services offered by libraries or educational institutions." http://www.fcc.gov/Reports/tcom1996.txt. By contrast, the term "Internet access service" in the CAN-SPAM Act of 2003, as stated in the Telecommunications Act of 1934, as amended, reads: "The term 'Internet access service' means a service that enables users to access content, information, electronic mail, or other services offered over the Internet, and may also include access to proprietary content, information, and other services as part of a package of services offered to consumers. Such term does not include telecommunications services." http://www4.law.cornell.edu/uscode/html/uscode47/usc_sec_47_00000231----000-.html.
[xliii] Geist, "Untouchable," *supra* note 8, at 17 (for a discussion of civil and criminal sanctions common in anti-spam legislation.
[xliv] For discussion of the effectiveness of such a measure, *see* Prince, "How to Craft an Effective Anti-Spam Law," *supra* note 1, at 9.
[xlv] http://www.icpen.org/.
[xlvi] For discussion of the effectiveness of the state of Washington's use of such a measure in the United States, *see* Prince, "How to Craft an Effective Anti-Spam Law," *supra* note 1, at 6 and 10.
[xlvii] For the full text of the Australian Telecommunications Act of 1997 that contains such provisions, *see* http://www.austlii.edu.au/au/legis/cth/consol_act/ta1997214/s117.html *et seq*.
[xlviii] The Australian Direct Marketing Association (ADMA) has also established a Code of Conduct. Where such an organization exists, such a code is another logical, parallel step; many countries will not have such an entity in place, in which event a legal provision mandating a parallel process of this sort would not make sense.
[xlix] Consider the findings of the New Zealand regulators with respect to the most effective mode of enforcement: "A civil penalty regime where the emphasis is on ISPs/carriers taking action in response to customer complaints is considered to be the best approach. This is because most spam in New Zealand originates from overseas and the ISP/carrier will often best be placed to put in place the appropriate technical measures to deal with it. In addition, if spam is originating from an address/number hosted by another ISP/carrier in New Zealand, then the user's ISP/carrier can approach the sender's ISP/carrier and seek action by that ISP/carrier against the sender. If complaints cannot be satisfactorily resolved in this way then the user's ISP/carrier can forward the matter on to the enforcement agency to consider whether an investigation or further action is appropriate." Ministry of Economic Development (NZ), "Legislating against Unsolicited Electronic Messages Sent for Marketing or Promotional Purposes (Spam) - Enforcement Issues - Cabinet Paper," at http://www.med.govt.nz/pbt/infotech/spam/cabinet/paper-two/paper-two-03.html#P31_3192.
[l] *See* http://www.truste.org/.

[li] Countries might consider also establishing a scheme for arbitrating disputes between consumers and ISPs that are the source of spam. In a related scheme, some countries have established consumer arbitration mechanisms to resolve disputes between telecom customers and their service providers. Spain's arbitration mechanism also includes a certification. *See* the ITU's 2002 Feedback to Regulators case study at http://www.itu.int/ITU-D/treg/Case_Studies/index.html.

[lii] The process underway at the Messaging Anti-Abuse Working Group may well provide extremely useful guidance on this front, both as a matter of process and of substance. *See* http://www.maawg.org/news/maawg050711.

[liii] *See* http://www.ftc.gov/os/2004/10/041012londonactionplan.pdf. *See also*, for particular suggestions, http://www.ftc.gov/bcp/conline/edcams/spam/zombie/index.htm. For a letter sent to 3,000 ISPs, as part of this initiative, *see* http://www.ftc.gov/bcp/conline/edcams/spam/zombie/letter_english.htm.

[liv] The specific suggestions for such zombie-prevention measures will vary over time. Some initial recommendations, derived as part of the London Action Plan meeting and related efforts, include: 1) blocking port 25 except for the outbound SMTP requirements of users authenticated by the ISP to run mail servers designed for client traffic and other carefully accredited purposes; 2) exploring implementation of Authenticated SMTP on port 587 for clients who must operate outgoing mail servers; 3) applying rate-limiting controls for email relays; 4) identifying computers that are sending atypical amounts of email, and take steps to determine if the computer is acting as a spam zombie. When necessary, quarantining the affected computer until the source of the problem is removed; 5) providing, or pointing customers to, easy-to-use tools to remove zombie code if their computers have been infected, and provide the appropriate assistance; and, 6) the shutdown of open relay servers after appropriate notice and inquiry. Regarding the first of these suggestions, related to port 25, Industry Canada (in a separate context), recommends, "ISPs and other network operators should limit, by default, the use of port 25 by end-users. If necessary, the ability to send or receive mail over port 25 should be restricted to hosts on the provider's network. Use of port 25 by end-users should be permitted on an as-needed basis, or as set out in the provider's end-user agreement / terms of service." http://e-com.ic.gc.ca/epic/internet/inecic-ceac.nsf/en/gv00329e.html.

[lv] The New Zealand regulators note: "The enforcement agency would be seen as also having a role in educating users/consumers on how to deal with spam in conjunction with the industry as well as a role in educating business and other organisations on how to comply with the legislation along with the Ministry of Economic Development, which will be responsible for administering the legislation, and organisations such as the Direct Marketing Association." Ministry of Economic Development (NZ), "Legislating against Unsolicited Electronic Messages Sent for Marketing or Promotional Purposes (Spam) - Enforcement Issues - Cabinet Paper," *supra* note 47, at http://www.med.govt.nz/pbt/infotech/spam/cabinet/paper-two/paper-two-03.html#P31_3192.

[lvi] For a description of open mail relays and their importance to the spam issue, *see* http://en.wikipedia.org/wiki/Open_mail_relay.

[lvii] For a definition of botnet, *see* http://en.wiktionary.org/wiki/botnet.