7 STEMMING THE INTERNATIONAL TIDE OF SPAM

Author: John G. Palfrey, Jr., Executive Director, Berkman Center for Internet & Society and Clinical Professor of Law, Harvard Law School

The anti-spam laws enacted around the world so far have been largely unsuccessful in stopping spam.[1] In almost every instance, anti-spam statutes have been directed at sanctioning spammers for their bad acts. An increasing number of countries and other jurisdictions have created such laws or applied to spam their existing, generally applicable laws concerning data protection, consumer protection, and protection against fraud. Yet, in many cases, these laws have missed their target entirely, with no perceptible impact on actual spammers. Even worse, the laws have often had negative side effects, in the form of transaction costs, administrative costs, and a chilling effect on legitimate senders of e-mail.

No matter what kind of law is enacted or applied, anti-spam measures require well-conceived, targeted, and coordinated enforcement mechanisms in order to be effective. Without a doubt, anti-spam investigations are invariably complicated and expensive, presenting challenges for any country seeking to enforce anti-spam laws. Even the U.S. Federal Trade Commission, with its substantial resources, 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 nearly meaningless because of the enforcement challenge.

Cross-border cooperation and enforcement is not only desirable, but also essential to spam fighting. But the variety of anti-spam laws and underlying legal systems on the books of various countries makes collaboration extremely difficult. The challenge of fighting spam through law – to be sure, only one of the potential modes of regulation – calls for new thinking and increased emphasis on international harmonization and collaboration. The only effective means of combating spam is likely to be a combination of approaches. As noted in the Chairman's report of the ITU 2004 Global Symposium for Regulators (GSR),[2] a multi-pronged approach to dealing with spam is an appropriate measure.

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 chapter takes up the elements that might be included in an anti-spam law. Second, it 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). Third, the chapter also examines a variant of the legal approach where ISPs are formally encouraged by regulators to develop their own code of conduct. 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.

7.1 The Spam Problem

The problem of spam is well established. The extent of the problem is plain to anyone who relies upon electronic mail (email) for communications. Email and related forms of messaging such as "blogs" (short for "Web logs") and short messaging service (SMS), have become an important and popular means of communication in cultures around the world. These services are cheap, they have global reach, and they are playing a key role in the development of e-commerce. The proof of their value is found in their 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, Outblaze, Yahoo! Mail, Google's Gmail, Wanadoo or Noos in France, among others).

But the openness that has made e-mail and its close cousins such tremendously easy ways to connect is also emerging as their greatest vulnerability. A combination of economics, technologies, and online behaviour norms has made the incremental cost of sending a spam message nearly zero, while promising senders a profitable potential return.

At first glance, the economics seem baffling. How can it possibly be worthwhile to send out grammatically challenged messages about low-cost pharmaceuticals or pirated software – offers that the vast majority of recipients ignore and quickly transfer to their "junk mail" folders? Part of the answer is the tiny marginal cost of sending spam messages. Because they cost nearly nothing to send, the response rate does not need to be very high. And it turns out that enough people *do* respond to make the endeavour worthwhile to the spammer. Astonishingly, the Business Software Alliance (BSA) has found that 22 per cent of British consumers they surveyed purchased software through spam.[3] Rates for the other five countries BSA surveyed were similarly high. The bottom line is that spam persists because it is profitable. Unless enough consumers become educated to avoid or reject spam, the best way to reduce spam may be to raise the risks and costs to the spammer.

Right now, the costs seem to be landing on consumers. Every 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.[4] The costs of this scourge are borne not by the spammers, but by those who run networks, employers and the individuals who receive the messages. Spammers – and those who use spam to perpetrate related frauds – take advantage of the open design of IP networks to render e-mail costly and nearly unusable for some businesses and consumers.

7.1.1 Legislative Responses

The "extremely rapid growth" of spam[5] has led to the enactment of more than 75 specific laws,[6] such as the well-regarded Australian law, the United States' CAN-SPAM Act of 2003 and comparable legislation in several dozen countries around the world.[7] These laws have, to date, been unable to stop spam. 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.[8] In fact, most indicators point in the other direction.[9]

Spam is best viewed not as a nuisance, but in the context of cybersecurity. Spam is bad enough as a drain on productivity and a daily annoyance. But few people consider that spam is enormously costly to 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" and "pharming,"[10] scams with endless permutations, and advance fee frauds, to name a few.[11] Spam is also undercutting the efforts of developing countries to persuade new users to rely on digital communications.

Bill Gates, who is arguably the world's most powerful technologist, 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.[12] He is not alone in having fallen short in this goal. In fact, most major, well-intentioned ISPs and e-mail service providers, along with many technology start-ups, have devoted many millions of dollars to 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 cooperate 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-level computer crime and common law statutes. This has resulted in multi-million-dollar judgments and settlements against "spam king-pins" who abuse their networks.[13] Microsoft won a USD 7 million judgment that may well have put an end to one spamming operation that allegedly distributed more than 38 billion unsolicited messages per year.[14]

These lawsuits – although 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. Indeed, the success of these efforts suggests that ISPs could become the most valuable players in the effort to end spam. The challenge for lawmakers is how to create a fair, effective regulatory regime that takes advantage of ISPs' ability to help end spam without placing an undue burden on law-abiding companies.[15]

7.1.2 A Model Law: One of Several Ways To End Spam

7.1.2.1 A Combination of Approaches Is Needed

The persistence of spam problem has led policy-makers, technologists, academics, and many others to come up with a wide range of possible strategies to end it. The least intrusive approach, most consistent with the end-to-end principle of network design, is to leave the job to end users, through simple technologies such as spam filters on e-mail clients. The improvement of authentication, accreditation, and identity management technologies ought to help make user-level controls more effective over time.[16] At Davos in 2004, Mr. Gates described Microsoft's pursuit of solutions to complement these user controls.[17] One approach calls for a combination of law, code, markets, and norms.[18]

Meanwhile, the chairman's report of the ITU Thematic Workshop on Countering Spam in 2004 contains a range of proposals, suggesting an intersection of many methods of spam-fighting.[19] 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 among ISPs, mobile carriers and direct marketing associations;
- The education of consumers and industry players about anti-spam measures and Internet security practices; and,
- International cooperation among government, industry, consumer, business and anti-spam groups, for a global and coordinated approach to the problem.

In fact, virtually every major report on spam calls for a combination of approaches to combat the problem, rather than a single, "silver-bullet" solution. This chapter does not take up in detail each of these anti-spam tools, but rather focuses on legal strategies, emphasizing those that are relevant to developing countries.

Anti-spam laws are perceived today to be a necessary tool for all countries, if for no other reason than that they help facilitate international cooperation in combating spam. Even the most ardent supporters of user controls and market solutions agree that governments have a role to play in tracking down and punishing the worst offenders, such as those who use spam to commit fraud. The existence of interoperable anti-spam laws creates a common baseline for international enforcement. A developing country may not be able, by itself, to enforce its anti-spam law, but that law can provide the basis for regional and multinational enforcement actions.

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.

7.1.2.2 The Effect on Developing Countries

Spam is arguably a bigger problem in developing countries than in wealthier countries, where anti-spam mechanisms are more robust. Many developing countries do not yet have anti-spam laws,[20] and those that do often do not have resources to enforce them.[21] Meanwhile, the effects of spam are often relatively more costly in developing countries. ISPs are frequently deluged by spikes in spam, which lead to network slowdowns and breakdowns.[22]

Moreover, many people in developing countries send emails from shared Internet connections and equipment, such as at cybercafés or other public access centres. These services ordinarily rely on hosted email services with limits on inbox sizes. Accessing email becomes too expensive if per-minute charges paid to cybercafé 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.

Officials from developing countries often point to the fact that most spam still comes from the United States and other wealthy countries, which have done little to help developing countries cope with the problem. In addition, they note that the resources of regional bodies such as the OECD are not consistently available to developing countries. This leaves them at a comparative disadvantage in fighting spam.

The answer for developing countries is not simply to copy anti-spam laws enacted in developed countries. That approach is unlikely to be effective. Anti-spam laws aimed at sanctioning spammers may be of little use in developing countries if the spammers are outside their jurisdiction. The challenge is to tailor legislation to patterns of usage in developing countries and to consider all avenues to combat spam, such as implementing enforceable codes of conduct for ISPs.

7.1.3 An Alternative Mechanism: Enforceable Codes of Conduct

In addition to enacting anti-spam legislation, developing countries could require ISPs to establish an industry code of conduct on spam. The enabling legislation for such a code could stipulate that the nation's regulatory agency would enforce the code against any ISP that materially violated it.[23] Such a proposal cuts jarringly across the grain of most internet regulation to date. As essential players in developing ICT-powered economies, ISPs have generally been left alone by legislatures, administrative agencies, and judges. They may be licensed and overseen by regulators in some contexts, but ISPs have largely been immune from prosecution for bad acts committed by people through their services.

7.1.3.1 Elevating the Role of the ISP

Ideally, it is not an ISP's job to be a gatekeeper. The ISP should pass all packets from sender to receiver, with end users deciding what to send and what to receive. Any departure from this model should be undertaken only when serious circumstances warrant it. In addition, regulation should be handled with a light touch, and any burdens placed on ISPs should not be starting points for more intrusive regulation.

It is essential to acknowledge how 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, and they 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. 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 it is no longer fully reflected in reality. A large number of control points have been built into the network – often to deal with massive problems like spam.[24]

ISPs still enjoy broad immunities in many jurisdictions from claims based on what others do on their networks. For example, they rarely face copyright violation or defamation claims. But they are increasingly called upon to play a role in protecting and policing the internet. There are substantial risks associated with placing such jobs in the hands of ISPs – particularly to civil liberties – so any legislation that mandates a greater supervisory role must be carefully drafted so as to mitigate these risks.

7.1.3.2 Establishing an Industry-Led Approach

Countries should work to establish an industry-led regulatory approach that provides a mechanism for regulators to step in against the worst spam abusers. This proposal is not meant to presage a wholesale shift in the role of ISPs. Nor is it meant to indicate a rejection of 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 burden ISPs further, especially given the constraints they already face.[25]

Rather, the goal is to reduce spam in a way that protects responsible ISPs. 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 behaviour. One means of rewarding those responsible ISPs is for regulators to hold their irresponsible competitors accountable. This would create a level playing field for responsible ISPs.

ISPs are no strangers to fighting spam. ISPs around the world have taken an active role in attacking spam at the source, before it clogs their customers' inboxes. Anti-spam measures implemented by ISPs cover a wide range. Many ISPs participate in industry-wide working groups, such as the Messaging Anti-Abuse Working Group.[26] Many also work with standard-setting organizations developing technical solutions.[27]

ISPs' initiatives are often geared toward improving security and decreasing the vulnerability of users and of their networks. When they succeed, it can often be a strong selling point for them. For example, Google's Gmail, a free Web-based e-mail service, removes hyperlinks from messages that the service believes to be phishing attempts.[28] The large U.S.-based ISP Earthlink requires all e-mail messages to be routed through its mail servers, in order to reduce the impact of "zombie" networks. Earthlink also mandates that users' e-mail programs submit passwords to transmit messages.[29]

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. End users may not update their own virus software automatically or regularly. Or, they may download programs that contain "malware" and "spyware" that compromise their computers, posing a risk not only to themselves but to other users worldwide, since their PCs may be hijacked to relay spam to other unsuspecting consumers.

Governments and ISPs both have incentives to end spam.[30] ISPs bear a large amount of the cost of spam and get nothing in return – unless they are charging a premium to spammers in exchange for sending spam out on their behalf. ISPs also are relatively close to the problem. After all, spammers need ISPs to get access to the internet to dump their messages. While spammers are increasingly sophisticated in evading tracking, a concerted effort among cooperating ISPs (and possibly law enforcement officials and end users) can find the worst offenders. The routing of spam can be traced and mapped at a network level.[31] While ISPs are often short on cash flow, many do have the financial and human resources to play a key role in the anti-spam fight.

National laws can mandate the development of codes of conduct by and for ISPs. Adherence to the code could be a licence condition, or it could be implemented through a rule-making proceeding, 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 with industry participation. The law would give ISPs the first opportunity to craft the code, outlining acceptable behaviour for ISPs and their customers. Preferably, the code would prohibit spam, phishing, spoofing on the ISPs network, and similar practices. It could also suggest or endorse the best use of spam filters and other technological tools for customers and ISPs to fight spam. The regulatory agency would approve and, in many cases, enforce the code.

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 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.

An enforceable code of conduct is not without drawbacks. The code must be narrowly tailored to curb spam and related bad acts. It should not be used as a back-door measure to overburden ISPs, such as by:

- Imposing anti-spam obligations where no technical solution yet exists (as with many anti-spoofing requirements);
- By using anti-spam measures as a means to limit legitimate political discourse or other protected speech; or
- By infringing on the privacy interests of citizens.

It is essential that the industry develops and approves the code of conduct – or, at a minimum, collaborates with regulators in this task. Industry "buy in" is important, because the code will require frequent updating to reflect new developments in spamming practices and anti-spam technologies.

7.1.3.3 Voluntary Codes of Conduct

As an alternative to a mandated code, enforced by regulators, governments might encourage ISPs to develop their own, industry-enforced codes of conduct. In fact, many ISPs are taking this step without any encouragement. Terms and norms are often built into "acceptable use" policies for customers and peering arrangements.[32] Under this voluntary model, regulators could advise the industry in developing the codes. It could then help consumers find the ISPs that have developed or signed on to those codes. If a vibrant ISP market emerges, consumers could then choose ISPs that have proactively tried to fight and reduce spam.

Finally, regardless of whether ISPs are compelled to establish codes of conduct or do so voluntarily, regulators have an important role to play in educating and raising awareness. Consumers, businesses, ISPs and cybercafé operators need information on technical solutions such as spam filters, as well as warnings about viruses and fraudulent activities that have been detected. There is much to be gained from government-industry collaboration in protecting consumers from spam.

7.2 An Outline of a Model Law

7.2.1 The Context for a Model Anti-Spam Law

Representatives of many countries, particularly in developing regions of the world, have sought a model law for combating spam. The topic was discussed intensively at two international gatherings hosted by ITU. The first, held in the summer of 2004, was devoted to the issue of spam, while the other, a year later, focused on cybersecurity. This chapter draws upon the many resources developed to date, in an attempt to create a model anti-spam law. There are multiple potential benefits of such a document:

- **Clear guidelines** – Email senders that want to comply with legal requirements could more easily learn what rules apply to them and could then follow them more consistently.
- **Jurisdictional Consistency** – Enacting a similar, model law in many jurisdictions would free ISPs and email senders from having 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 offences, 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 abuse of electronic communication, would strengthen norms that deplore such conduct.
- **Fewer havens for spammers** – As more governments adopted the model law, spammers would have fewer friendly locations to establish operations. This would increase their costs and reduce the financial incentives to engage in massive spamming.
- **Increased sharing of best practices** – Since legal systems would share harmonized provisions, regulators and enforcers could more easily collaborate to develop and share best practices for implementing spam laws.[33]

Even well-crafted anti-spam laws, implemented in every jurisdiction, will never get the job done alone. But anti-spam legislation can be a useful element of a coordinated anti-spam strategy. A good anti-spam law should distinguish between good actors and bad actors and mete out punishment accordingly. Moreover, if spammers were liable for each spam message they send, the level of fines would increase exponentially, according to the scale of the spam operation.[34] Enforcement is the key – and the most difficult element – particularly in developing countries.[35]

The development of a model anti-spam law should be collaborative and inclusive. As with any model law (or any official document with the force of law) an anti-spam law must be flexible enough to dovetail with existing laws, including anti-fraud, consumer-protection, telecommunication and internet-specific laws and regulations. One relevant example is the process that the United Nations Commission on International Trade Law (UNCITRAL) undertook in establishing its Model Law on Electronic Commerce (1996).[36] UNCITRAL's e-commerce model law does not specifically address spam, which did not exist as in 1996 as the huge issue that it is today. Anyone designing an anti-spam model law should also consider the broad range of laws on the books today in many countries, containing variations that are worth considering but that are too numerous to be included in this chapter.[37]

Most of the existing anti-spam laws are directed at controlling spammers' behaviour. This seems appropriate, since spammers directly cause the problem. But the current slate of laws has failed even to curb the *growth* of spam, much less to reduce the problem.[38] Why have they failed? Some observers argue that the countries generating the largest proportion of the world's spam have done too little at home to stop the problem.[39] Those making this argument especially criticize reliance upon "opt-out" rules that allow spam unless consumers specifically ask not to receive it. Even then, opt-out rules are not enforced aggressively enough.

It is not enough to blame the greatest spam-producing nations, though. No country in the world – including those lauded as the most effective in combating spam – has made significant inroads using classic enforcement mechanisms. Of course, it would help if governments updated their laws in

light of their apparent inadequacy, but that takes time. Other observers suggest that anti-spam laws should be focused not on the spammers themselves, but rather on the (often dodgy) companies for whom the spam is sent. [40]

The primary issue is that little emphasis is placed on investigation, enforcement powers, or resources. It is not that hard to build and win a case. Most spammers and their clients eventually can be found, with enough hard work and cooperation. The problem is that each investigation is so time-intensive and costly that police and prosecutors often decide that the costs outweigh the benefits. One of the core tenets of the model law described below is that it emphasizes creating a framework for national enforcement, international coordination, and distributed monitoring through the ISP code of conduct.[41]

7.2.2 Elements of a Model Spam Law

The draft model law presented in this section as an annotated outline roughly follows 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.[42] This section describes the key elements of a model law, offering suggestions for options at each stage of the drafting process.

One threshold issue is whether the law will be an "opt-in" or an "opt-out" statute. An opt-in statute makes it illegal to send spam unless a recipient has affirmatively agreed to receive it. Often, only tacit acceptance is required, such as the existence of an ongoing business relationship of some kind. An opt-out statute, on the other hand, permits spam unless the recipient has specifically informed the spammer that he or she does not want to receive it.

The decision to choose an opt-in or opt-out approach will reverberate throughout the law from that point onward. For instance, in an opt-out system, the provision to establish an "unsubscribe" function will be more essential and take on a different character than in an opt-in law, which presumes that the receiver already gave a green light before receiving any spam messages.

One deficiency of many spam laws is a lack of clear definitions. The draft model law, below, seeks to head off variations among definitions adopted in different jurisdictions, because these variations could undermine international cooperation on enforcement.

Draft Model Law

Section 1: Introduction and Definitions

The law should 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 the definitions, which take on special significance in the anti-spam context. On the one hand, the terms must be broad enough to encompass emerging types of spam as they develop. On the other hand, the provisions must be precise enough to be clearly understood. In addition, since anti-spam statutes can affect civil liberties such as free speech and personal privacy, definitions may play a pivotal role in determining whether the statute is permissible under a country's constitutional framework or sufficiently protective of citizens' rights.

The following are some of the key terms to be included in the definitions section of the model law, (although this is not a complete list):

- **Address-harvesting software.** The law should define what types of computer applications used to harvest e-mail addresses are banned 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, technologies that support spamming, such as address-harvesting software. If such as ban is included in the 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 is not to ban any technology, but rather to bar its use for gathering e-mail addresses for spamming.

- **Authority, or Regulator.** The law should specify the entity or individual that has jurisdiction over the anti-spam law. Countries vary as to the precise placement of this authority, which might be vested in the telecommunication regulator, the consumer protection authority, the trade regulator, or another authority.

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

- **Authorization.** The law should clarify what it means for an individual to authorize sending a message that could be defined as spam.

  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," this definition might not be necessary.

- **Commercial.** The law must specify with precision what constitutes a message sent for commercial purposes. Commercial messages sent to recipients with whom they 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 variation in the treatment of speech rights in different countries. In Australia and the United States, for instance, legislators and regulators have stayed clear of regulating unsolicited political messages in light of constitutional protections 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 it applies only to commercial messages, but it is important to define what constitutes "commercial" in any event.

- **Consent (or, Affirmative Consent).** The law should clearly state what the recipient must do to signal willingness to receive e-mail from a particular sender. The law could use the term *affirmative consent*, which 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 another party for the purpose of initiating commercial electronic mail messages.

Annotation: This definition should *be coordinated with the definition of the term "authorization," as needed.*

- **Electronic message.** The law should specify what constitutes an electronic message. In the Australian statute, an electronic message is a message sent using (a) an Internet carriage service or (b) any other listed carriage service. Also, an email message is sent to an electronic address in connection with (1) an e-mail account; (2) an instant messaging account; (3) a telephone account; or (4) a similar account.

Annotation: An important area to consider is what applications the anti-spam statute covers. The best anti-spam laws will be general enough to cover ICT-based unsolicited messaging in formats that have yet to be devised, as well as those 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), spam over Internet telephony (SPIT), voice messaging over Internet telephony 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 which party bears the burden of producing evidence.

Annotation: One of the key problems that enforcement authorities face 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 receiving spam. Virtually no individual can prove the negative – that they never entered *into a commercial relationship, or never once hit "OK" in a click-through contract. 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 type of service the statute covers. The essential part of the definition is that the covered party 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 by various internet-related laws, so special care should be taken to harmonize definitions across statutes, for clarity's sake. U.S. law, for instance, has more than 40 potential definitions for terms that resemble "Internet service provider." [43] *The elimination of* ambiguity *is particularly important 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.

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. Countries vary widely in terms of whether messages beyond "unsolicited commercial e-mail" are included under 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 at which each country must decide whether to join the opt-in or opt-out camp. Virtually all anti-spam laws focus upon the act of sending (or attempting to send) as the core, operative offence. 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 sending the message.

Annotation: The law might also require that commercial email be identified as an advertisement, by requiring that "ADV" or the like be included in the header. The law could also require commercial email to include the sender's valid postal address. Some activists have also called for the requirement that senders label sexually explicit messages in the subject line. The labeling requirement is hotly contested by e-mail marketers, who fear that ISPs or individuals will filter out all such messages, even if they are legitimate commercial offers.

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

Commercial electronic messages must not include false information. That includes an email's "from," "to," and routing information, which should include the originating domain name and email address. 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. Without the general ban on unsolicited emails, this accuracy requirement can be criticized as effectively permitting spam that is unwanted but accurate. Much of the criticism leveled against the U.S. CAN-SPAM Act of 2003 has followed this 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" or opt-out facility. If a recipient exercises the right to request no further emails, the sender must be bound to honour that request. In an opt-in regime, an unsubscribe provision would basically ensure that any recipient who had previously opted in could reverse that decision and opt out at any time.

Annotation: In the United States, 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 honour that request. 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 allows 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 its behalf.

Also, 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 bolster spamming lists, since the spammers then know that the email has reached 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 general-purpose technologies. Any provision of this sort ought to 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, although in many jurisdictions such acts would be covered under statutes related to computer crimes, larceny, trespassing or other offences.

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

The main remedies for violation of the law would be civil penalties and injunctions. Criminal penalties, including imprisonment, are also sometimes sought when false representation, use of another's computer to perpetrate a fraud, or similar acts are involved.[44]

Annotation: The law might also include a provision making it a criminal offence 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 offence.

Section 8: Causes of Action

This section would establish a cause of action for regulators against anyone hiring a spammer to distribute bulk email 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, etc.)[45]. The law might also include additional causes of action, enabling ISPs, enforcement officers in lower jurisdictions, and harmed individuals to initiate cases.

Section 9: International Cooperation

The law should create a mechanism for international information sharing and, possibly, formal cross-border enforcement support. These rules would simplify the process for exchanging information and encourage exploration of memoranda of understanding (MOUs) 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 U.S. Federal Trade Commission has been encouraging the U.S. Congress to pass legislation to make such cooperation more likely to succeed. Consider also the work of the International Consumer Protection and Enforcement Network, which involves dozens of countries in "sweep days" to rid the internet of scams.[46]

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. The purpose is to protect the state's residents.[47] A list of that nature, held in one place, however, could 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 for ISPs.[48] Such provisions might include:

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

b) A provision granting regulators authority to require all ISPs to develop a code of conduct for that jurisdiction.

c) A description of the multi-stakeholder process involved in developing codes of conduct, including what groups will represent the interests of 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 draft a code of conduct in the event that industry cannot agree or otherwise fails to develop one.

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 (see Box 7.1). There are several issues to be considered, many of which are set forth in the section that follows. The law would need to establish a deadline for compliance and provide for periodic updating of the code. One option would be to task an industry association (if one exists in that jurisdiction) to develop the code. The next decision would be whether all ISPs have to comply with a code developed by the association. The enabling provisions for the code might allow ISPs to opt out of a code developed by the association and register a separate code with the regulator, provided the ISP's self-developed code sufficiently protects the public interest.

7.3 Codes of Conduct

The primary goal of a code of conduct is to ensure that ISPs that provide a route to the internet – the source ISPs – are taking adequate steps to keep spammers off the network. The effect of the code should be to level the playing field for ISPs that are actively seeking to rid the network of spam instead of profiting from sourcing it. While there are many risks in regulating ISPs more extensively than they have been in the past, a carefully balanced set of provisions will benefit not just customers, but all well-intentioned ISPs, too.[49]

In virtually all instances, industry knows better than most regulators what technical solutions to spam exist and can be implemented.[50] Regulators have a role to play in ensuring that industry does all that it can to put technical and policy solutions in place and to share best practices.

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. If combating spam is not in the remit of the telecommunication 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 legal codes, such as the telecommunication laws and regulations. The code of conduct does rely, however, upon core elements of an anti-spam statute.

7.3.1 Procedural Steps Toward an Enforceable Code of Conduct

Industry codes of conduct should be developed in a 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 process of drafting a code likely 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 enabling law or regulations. The process by which a code is drafted should be set forth in the law or regulations so as to ensure broad and open participation by key stakeholders.
- Where appropriate, the regulator can help by sharing best practices. This can be done, for example, through the use of ITU's Global Regulators Exchange (G-REX)[51] or face to face meetings such as ITU's annual Global Symposium for Regulators (GSR). Regulators may also be 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-antispam.org
- The relevant industry members present the draft 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 the industry fails to develop a code, or if the code is not deemed acceptable, the regulator has the power to step in to draft or revise it, ensuring that 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 monitor messages any more than they already do. The expectation is that ISPs would only need to take reasonable measures, such as investigating when they receive 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 end users' complaints against ISPs for failure to live up 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, harsher licensing requirements, or lawsuits.

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 experienced damage by spam or phishing could be given the right to go to court to sue ISPs directly for violating the code of conduct. Also, regulators *could require ISPs to include in their customer contracts binding agreements to honour the code. This would allow consumers and companies to sue not only under an anti-spam law, but also pursuant to laws governing breach of contract.*

- The code could also create a "certification" or "accreditation" system, allowing ISPs to publicly advertise their compliance with the code. The accredited ISPs would be able to display a "trust mark" signifying their status, helping consumers to make reasonable decisions about which service to choose.[52]
- The code should also include a mandatory review or "sunset" provision to ensure that the rules remain effective and appropriate in a fast-changing technological and legal environment.

7.3.2 Elements of a Model Industry Code of Conduct

Like a model law, an industry code of conduct should be developed in an inclusive, collaborative atmosphere, designed to elicit the best thinking from a range of experts and concerned stakeholders.[53] The code should set forth the responsibilities of ISPs and other actors with sensitivity to local concerns. But it should also take 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 correspond to the definitions in the enabling law.
- Procedures ISPs should follow in dealing with obvious spam that comes into the ISP's sub-network (including procedures relating to the provision or use of filtering software).
- A commitment not to serve individuals or companies that send unsolicited commercial email in bulk, and to terminate those clients when complaints and subsequent investigations reveal that they have been spamming through the ISP's network. This should also include a commitment to refuse payment, or any enticement of a premium payment, offered by a known spammer for any service.
- A commitment to give ISP subscribers information about the availability and use of software for filtering spam at the client level. ISPs should also commit to helping subscribers prevent their computers from being infected by worms, "Trojans" and other malware that turns computers into spam "zombies."
- A commitment to assist in developing and evaluating filtering software that gives end users a maximum level of control over what to accept and to reject.
- Suggested best practices that ISPs can implement, as appropriate, in order to minimize or prevent spam. At present, such suggested best practices might include some of those set forth in the London Action Plan.[54]

The London Action Plan stemmed from a July 2004 meeting of "government and public agencies from 27 countries responsible for enforcing laws concerning spam." They generated several recommendations affecting:

- The optimal configuration of servers and other network devices to minimize or prevent spam;
- A commitment to taking meaningful zombie-prevention measures;[55] and,
- A statement of principles for entering into peering arrangements only with ISPs that adhere to the full code of conduct.

The provisions of codes will no doubt change rapidly as the nature of the problem changes. Today, up to half of all spam is sent through "zombie" computers, suggesting that it is vital to help end users prevent the hijacking of their computers. Once this loophole is closed, spammers are sure to look for other mechanisms, and codes will have to be updated accordingly. The enabling law should be flexible enough to accommodate changes in the technological landscape.

7.3.3 Hazards of Enforceable Codes of Conduct

Adopting a regime of enforceable codes of conduct for ISPs is not without hazards. A well-designed policy, however, should be able to mitigate these risks, which are worth exploring here.

The purpose of industry codes of conduct should be to give ISPs incentives to exclude spammers from their networks, not to over-regulate ISPs. Nor should regulators use codes to deputize ISPs to overzealously block email or monitor conversations. Codes should be strictly limited to requiring ISPs to shut down spammers. They should not be employed for other objectives, such as shutting down email with what the government considers unpalatable political messages or for surveillance of a country's citizens. The risk is that empowering ISPs as gatekeepers will lead them to avidly look into the nature of messages sent across their networks.

This potential pitfall points back to the importance of defining spam in the anti-spam law. A properly crafted law should rule out abuses of authority in the name of preventing spam. Regulators should clearly focus on the goal of weeding out the worst, most obvious cases of spamming, rather than on pressuring ISPs to shut down legitimate e-mailers.

Another risk in establishing an enforceable code of conduct stems from political realities. In many countries, ISPs have enjoyed broad immunity from regulation and may oppose any spam-related responsibilities. More often, the ISP may be a monopoly, state-owned provider that generates important rev-

Box 7.1: Australia Telecommunications Act 1997 – SECT 117

Registration of industry codes

1) This section applies if:

a) the ACMA is satisfied that a body or association represents a particular section of the telecommunications industry or the e-marketing industry; and

b) that body or association develops an industry code that applies to participants in that section of the industry and deals with one or more matters relating to the telecommunications activities or e-marketing activities, as the case may be, of those participants; and

c) the body or association gives a copy of the code to the ACMA; and

d) the ACMA is satisfied that:

i) in a case where the code deals with matters of substantial relevance to the community-the code provides appropriate community safeguards for the matters covered by the code; or

ii) in a case where the code does not deal with matters of substantial relevance to the community-the code deals with the matters covered by the code in an appropriate manner; and

e) the ACMA is satisfied that, before giving the copy of the code to the ACMA:

i) the body or association published a draft of the code and invited participants in that section of the industry to make submissions to the body or association about the draft within a specified period; and

ii) the body or association gave consideration to any submissions that were received from participants in that section of the industry within that period; and

f) the ACMA is satisfied that, before giving the copy of the code to the ACMA:

i) the body or association published a draft of the code and invited members of the public to make submissions to the body or association about the draft within a specified period; and

ii) the body or association gave consideration to any submissions that were received from members of the public within that period; and

g) the ACMA is satisfied that the ACCC has been consulted about the development of the code; and

h) the ACMA is satisfied that the Telecommunications Industry Ombudsman has been consulted about the development of the code; and

i) the ACMA is satisfied that at least one body or association that represents the interests of consumers has been consulted about the development of the code; and

j) in a case where the code deals with a matter set out in paragraph 113(3)(f)-the ACMA is satisfied that the Privacy Commissioner has been consulted by the body or association about the development of the code before the body or association gave the copy of the code to the ACMA; and

k) the ACMA has consulted the Privacy Commissioner about the code and consequently believes that he or she is satisfied with the code, if the code deals directly or indirectly with a matter dealt with by:

i) the National Privacy Principles (as defined in the *Privacy Act 1988*); or

ii) other provisions of that Act that relate to those Principles; or

iii) an approved privacy code (as defined in that Act) that binds a participant in that section of the telecommunications industry or the e-marketing industry; or

iv) provisions of that Act that relate to the approved privacy code.

2) The ACMA must register the code by including it in the Register of industry codes kept under section 136.

3) A period specified under subparagraph 1) e) i) or 1) f) i) must run for at least 30 days.

4) If:

a) an industry code (the *new code*) is registered under this Part; and

b) the new code is expressed to replace another industry code;

the other code ceases to be registered under this Part when the new code is registered.

Note: An industry code also ceases to be registered when it is removed from the Register of industry codes under section 122A. http://www.austlii.edu.au/au/legis/cth/consol_act/ta1997214/s117.html

enues for the government, giving it substantial clout in policy councils. Again, it may resist any attempts to further regulate it.

Meanwhile, there are costs associated with any new administrative mechanism, even one as simple as the development, registration, and updating of a code of conduct. Potential costs should be factored into the cost-benefit analysis when considering adopting such a regime.

Additionally, 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 see sufficient incentives to do so. ISPs often have to balance multiple interest and desires regarding spam, including:

- A desire to attract and retain bad-acting but paying customers,
- A desire to avoid the cost of transmitting spam through their networks, and
- A desire to avoid the regulatory risks and costs of transmitting spam.

ISPs may over-enforce the provisions of their own code, resulting in messages not getting delivered to recipients. This would be a far worse outcome, many argue, than dealing with the current deluge of spam. ISPs may also not be as sensitive to the rights of free expression, and most speech protections do not extend to non-state actions, often allowing private actors to block otherwise protected speech.

Meanwhile, ISPs would likely pass anti-spam 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. Cost concerns, however, should be seen in the context of the spam problem itself, which is adding to the cost of internet access and helping criminals to perpetrate fraud and disseminate destructive viruses. These network ills are bad not only for consumers, but for ISPs themselves.

Any legal and regulatory approach should seek to mitigate these drawbacks. On balance, however, many jurisdictions will likely find enforceable codes of conduct to be a sound policy choice, because they distribute part of the enforcement burden to stakeholders closest to the source of the spam problem – the ISPs and the end users.

7.4 Education and Awareness

The ideal solution to spam would involve no new law whatsoever. If consumers and businesses could take spam fighting into their own hands, the problem would be solved at the lowest cost and at the quickest rate. The brunt of anti-spam enforcement would be borne at the furthest edges of the network and in the most distributed manner possible. Those who pay the true costs of spamming – the end users – would ideally take the lead in combating spam, while regulators focused their enforcement resources on the largest, most complex cases.

Regulators would still have an important role to play, however, in educating consumers, businesses and ISPs about the dangers of spam and the steps they can take to protect themselves against it.[56] The London Action Plan includes some suggestions:

- Regulators should develop a plan for consumer and ISP education, posting information on their websites and developing print materials for distribution to cybercafé owners, consumers, businesses and ISPs.
- Regulators should provide a simple method for consumers to make complaints about spam.
- Regulators should create a special "combating spam" page on their websites, providing information about anti-spam practices and products. The web page should host practical advice on spam filters, warnings about phishing attempts, viruses and scams carried out using e-mail and other important tips for consumers. Examples of websites 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 et des Libertés in France (CNIL République Française): http://www.cnil.fr/index.php?id=1539
  - Guidance provided by the Korea Spam Response Centre of the Korea Information Security Agency, an affiliated agency of the Ministry of Information and Communication: http://www.spamcop.or.kr/eng/m_3_2.html
  - The United States' Federal Trade Commission's spam education pages: 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 take an enforcement role. The regulator can also help educate ISPs about some relatively simple technical measures. Specific measures include the latest information related to the blocking of open relays,[57] focus on "botnets,"[58] and slowdowns of traffic on port 25 that might make an enormous difference, particularly in developing countries.

Consumer and ISP education is a necessary component of spam-fighting strategies, but efforts in this field have had little effectiveness to date. This is not due to any fault in the outreach techniques themselves, but rather due to the limited vigour with which they have been pursued. It is challenging to communicate technical information to a lay audience. Moreover, education efforts cannot succeed in isolation, without other effective technological and regulatory measures. Substantially greater efforts in this area are warranted and would pay large dividends.

7.5 Conclusion

Despite the challenges that are bound to lie ahead, regulators should encourage the adoption of an anti-spam law that is harmonized, as much as possible, with those of other countries. Such an anti-spam law might involve creating an enforceable code of conduct for ISPs, placing the responsibility for mitigating spam closer to where the technical expertise lies. The problem with anti-spam laws enacted to date is that they have failed to create an enforceable regime or to bridge the divide between governments and the technologists who have the real expertise to solve the problem. While it is an imperfect remedy, an enforceable code of conduct could help to erase the shortcomings of earlier anti-spam laws.

The effort to fight spam is not going to succeed through pursuit of any one, single strategy. Success will be based on international cooperation and a range of shared strategies, including legal and regulatory mechanisms, technical improvements, market forces, and consumer-oriented solutions. The development of ISP codes of conduct, and their enforcement by regulators, can help stem the tide of spam and materially reduce spam's costs to ISPs and consumers.

[1] 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.").

[2] http://www.itu.int/ITU-D/treg/Events/Seminars/2004/GSR04/index.html

[3] 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.

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

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

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

[7] 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.

[8] AOL claims that spam is down 85 per cent 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. *See also* http://www.washingtonpost.com/ (27 December 2004). 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.

[9] 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.

[10] "Phishing" refers to a scam in which perpetrators send an email purporting to be from a legitimate business (such as a bank) and ask recipients to provide personal (often financial) information. Victims believe they are complying with a bona fide request, when they are being tricked into providing information to thieves. "Pharming" refers to a scheme in which victims clicking on a website are unknowingly diverted to a duplicate or fake website, where they can be fleeced.

[11] *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).

[12] http://news.bbc.co.uk/2/hi/business/3426367.stm.

[13] The AOL legal department posts decisions and litigation to their website 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).

[14] *See* http://abcnews.go.com/Technology/PCWorld/story?id=1029922&ad=true.

[15] This discussion paper 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.

[16] 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).

[17] BBC, *supra* note 10.

[18] 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).

[19] *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.

[20] *Ibid.*, point 24 at 4.

[21] 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.

[22] *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.

[23] *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.

[24] *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.")

[25] *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).

[26] http://www.maawg.org/about/roster/

[27] 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/).

[28] *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.

[29] *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.

[30] 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/).

[31] As one illustration of the fact that spam can be traced, *see* http://www.channelregister.co.uk/2005/09/20/spam_map/.

[32] Consider, for instance, that MAAWG is already promoting industry-wide codes of conduct. *See* http://www.maawg.org/about/.

[33] Bambauer, Palfrey, and Abrams, "A Comparative Analysis of Spam Laws: the Quest for Model Law," *supra* note 9, at 11.

[34] Prince, "How to Craft an Effective Anti-Spam Law," *supra* note 1, at 4.

[35] *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."

[36] Accessible online at http://www.uncitral.org/pdf/english/texts/electcom/05-89450_Ebook.pdf.

[37] *See* http://www.itu.int/osg/spu/spam/ for a catalogue of existing anti-spam laws on the books in jurisdictions around the world.

[38] 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.

[39] *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 per cent of the world s spam).

[40] *See* the FAQ page for the Coalition Against Unsolicited Commercial Email, at http://www.cauce.org/about/faq.shtml#offshore.

[41] 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.

[42] 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

[43] 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.

[44] Geist, "Untouchable," *supra* note 8, at 17 (for a discussion of civil and criminal sanctions common in anti-spam legislation).

[45] For discussion of the effectiveness of such a measure, *see* Prince, "How to Craft an Effective Anti-Spam Law," *supra* note 1, at 9.

[46] http://www.icpen.org/.

[47] 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.

[48] 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*.

[49] 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.

[50] 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.

[51] G-REX is an online discussion platform reserved for policy-makers and regulators> For more information, see: http://www.itu.int/ITU-D/grex/index.html.

[52] *See* http://www.truste.org/.

[53] The process under way 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.

[54] *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.

[55] 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.

[56] 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.

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

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