DISCUSSION PAPER

COUNTERING SPAM:

HOW TO CRAFT AN EFFECTIVE ANTI-SPAM LAW

International Telecommunication Union

This paper has been prepared for the ITU World Summit on the Information Society (WSIS) thematic workshop on Countering Spam, organized under the ITU New Initiatives Programme by the Strategy and Policy Unit (SPU). The paper was written by Matthew B. Prince, CEO and co-founder of Unspam, LLC, a Chicago-based business and government consulting company helping to draft and enforce effective anti-spam laws. He is a member of the Illinois Bar and an Adjunct Professor at the John Marshall Law School. He received his J.D. from the University of Chicago Law School and his B.A. from Trinity College, Hartford, Connecticut. For more information visit: http://www.unspam.com/.

The meeting project is managed by Robert Shaw (Robert.shaw@itu.int) and Claudia Sarrocco (claudia.sarrocco@itu.int) of the Strategy and Policy Unit (SPU) and the series is organized under the overall responsibility of Tim Kelly, Head, SPU. This and the other papers in the series are edited by Joanna Goodrick.

1 Introduction

Since the first anti-spam law worldwide was passed in 1997, at least 75 governments around the world have passed anti-spam laws.[1] That first anti-spam law was in fact passed at state-level in the United States, by the state of Nevada.[2] The anti-spam laws in existence today take the form of so-called "opt-in" or "opt-out" regulations. Some require labels or other markings to identify certain messages as unsolicited or pornographic. Others punish senders who use fraudulent or deceptive techniques. Still others require the sender to provide his or her identity and a mechanism to remove the recipient from future mailings. A survey of anti-spam laws around the world shows that the tools lawmakers have used to regulate spam are varied. Unfortunately, the one common trait they share is that almost all have failed to effectively tackle the problem, which has persisted beyond all legal countermeasures. An effective approach has yet to be found, but a deeper enquiry into how to create an effective law is more valid than ever before.

The empirical evidence for the failure to date is quite clear. Since the enactment of the first anti-spam law, spam has grown from a mere nuisance into a global plague. In 1997, the average e-mail user received approximately one unsolicited commercial e-mail message per week.[4] By 2003, the average e-mail user received 25 such messages daily.[5] While that is an astounding 175-fold increase in merely six years, the averages vastly understate the problem for many active e-mail users, some of whom receive literally thousands of spam messages each day.[6] Spammers routinely flout the law because the risk of prosecution is so low. Three months after the passage of a national anti-spam law in the United States, known as the CAN-SPAM Act,[7] only three per cent of spam messages complied with its requirements.[8] What is worse is that today the compliance rate is down to a scant one per cent.[9]

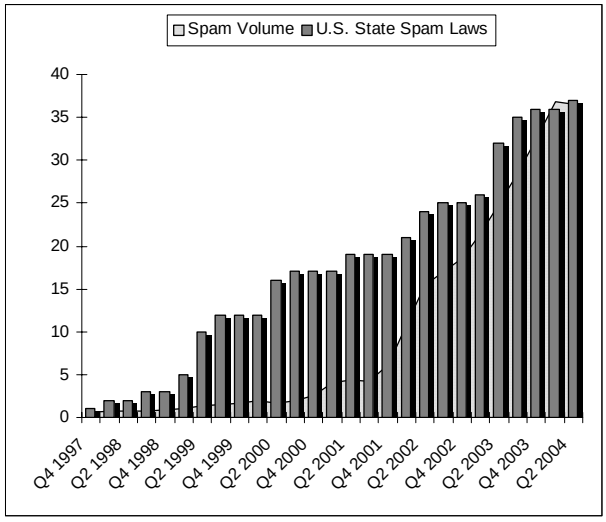

Figure 1. Thirty-seven states in the United States have passed anti-spam laws since 1997. In spite of a variety of regulations, including both opt-in and opt-out approaches, the laws have had little effect on the growth of the overall spam volume.

The near-viral growth of spam comes not only in spite of the passage of more than 75 anti-spam laws around the world, but also the extensive use of filtering technology which was unheard of in 1997.[10] Filtering and other technological measures have, to this point, been a double-edged sword. While there is no doubt that filters have become better at blocking unwanted messages, the total number of messages getting through to recipients' inboxes has, in many cases, continued to rise. This rise can be explained by the fact that sending spam is a business with virtually zero incremental costs.[11] As a result, even as filters have increased in accuracy, spammers have been able to simply inflate their total volume. The consequence is often that the same number of messages get through to recipients without spammers facing substantial additional costs.[12] Often described as an "arms race" between filter makers and spammers, today's situation can also be seen as a chicken and egg problem: spammers send more messages because there are more filters, and there are more filters because spammers continue to send more messages. The true casualties of this cycle are those businesses and organizations that cannot afford—for financial or practical reasons—to install rigorous filtering systems. They are caught dealing with the full force of the spam tsunami, and they are literally drowning.

It is important to remember the incredible efficiency e-mail delivers. Technological advances have virtually eliminated the marginal costs from e-mail communications. Although this is a remarkable accomplishment, it means a few individuals can exploit this efficiency to create the worldwide problem of spam.[13] Examining the basic economics of spam, it quickly becomes clear that the solution to this problem almost certainly begins by imposing increased marginal costs on spammers as they send each message.[14] The clearest example of such a proposal is e-postage.[15] The idea of e-postage is to make e-mail slightly less efficient for all users in order that it will become too expensive for spamming to continue to exist. But it should give us pause when a solution being proposed involves adding inefficiencies for nothing more than inefficiency's

sake. We should worry when the solution to spam is to impose transaction costs on a virtually transaction-cost-free environment. And while someday some form of e-mail postage may be necessary for us to internalize the costs of spam, we need to be extremely careful not to destroy what is the inherent magic of e-mail.

Effective anti-spam law, however, can be like e-postage that only spammers are required to pay. This is why, in spite of early failures, there should remain hope that law can do some good. While it is foolish to believe that law alone will ever completely eliminate spam, the law is particularly good at imposing costs. Moreover, a well-crafted law can 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.

In order for the risk to be credible, however, the law must be regularly and successfully enforced. Regrettably, to this point none of the world's anti-spam laws can claim this distinction.[16] Until we understand the factors that have kept this first generation of laws from success, it will be impossible to design the next generation to more effectively address the spam problem. When passing anti-spam laws, we need to stop simply repeating what has been tried and failed already. We need a framework to evaluate and understand the likelihood of a new law's success. We need to draft measures that actually assist law enforcement, foster international cooperation, generate revenue to fund prosecutorial taskforces, and drive down the costs of tracking and prosecuting spammers. Until we do this, spammers will continue to ignore our laws because our laws will continue to pose no threat to them.

2 Sentiment versus action laws

To date, the vast majority of the laws passed to regulate spam have been what can be called, for the purposes of this paper, "sentiment laws." Sentiment laws are designed to send a message about a community's sentiment (*e.g.*, "we, as a community, oppose unsolicited commercial communications") but put little effort or design into how they will actually be enforced. Sentiment laws tend to work well only in situations where there is no moral ambiguity, or the problem is in a nascent enough stage that the law can steer public opinion. Moreover, sentiment laws are inappropriate in instances where a few actors can, with relatively low cost or effort, cause widespread problems. This is because it is inevitable that at least a few individuals will always resist or ignore the community's norms. If their actions alone are enough to cause a widespread social problem, the law will need to bring more to bear than the community's sentiment in order to deter them.

This is not to criticize sentiment laws. In fact, these laws in certain circumstances can be extremely effective. For example, anti-incest laws are generally followed even though they provide little more than the community's sentiment.[17] Moreover, many murder laws are basically sentiment laws. Murder laws are effective in large part because they express a universally agreed-upon community norm. They also regulate what is, while a horrible crime, an act that is typically limited in scope and duration.

Compare on the other hand the laws many countries have enacted to combat terrorism. These anti-terrorism laws tend to focus not on the undeniable moral outrage over the act, but instead on empowering law enforcers with the special tools and powers necessary to stop the crime.[18] Laws against terrorism are not sentiment laws; they are what can be called "action laws". They aim to solve the practical problems law enforcement authorities face when trying to stop the crime of terrorism. Terrorism inherently is a crime where the law-breakers do not follow society's moral code and where a limited number of individuals can cause widespread problems. As a result, laws that simply express the public's sentiment would be unlikely to provide much, if any, deterrent effect.[19] Instead, anti-terrorism laws often grant broad subpoena powers, fund prosecutorial taskforces, and lower evidentiary standards with the purpose of making the apprehension and prosecution of terrorists less difficult.[20]

Using this analogy to understand the problem of drafting effective anti-spam legislation, the following can be affirmed: laws against murder are to laws against terrorism as current laws against spam are to effective laws against spam. It should be clear here that this analogy is not intended to draw moral equivalence between the crimes of murder or terrorism and spamming. Rather, it is under the view that understanding the core difference between sentiment laws and action laws can help us design more effective anti-spam legislation. Put another way: if law is going to have any positive effect on the problem of spam, then we need to move

from sentiment laws that simply express the fact that we do not like unsolicited e-mail to action laws that empower law enforcement authorities to do something about it.

3 Opt-in, opt-out, opt-up, opt-down

The focus of most discussions over anti-spam law to this point has revolved around "opt-in" versus "opt-out" approaches. The difference between these two philosophies of anti-spam law is easy to understand, although not nearly as relevant as it has been made to seem. Governments that adopt an "opt-in" approach announce to the world their sentiment that marketers should not send messages to a recipient unless the recipient has affirmatively asked to receive them. Under most opt-in laws, affirmative requests for messages may be delivered directly by a recipient in the form of an actual request or they can be constructively construed if the sender has an existing business relationship with the recipient.[21] For example, if you purchase a product from a merchant, under most opt-in laws that merchant may send you offers in the future until you ask to no longer receive them.

On the other hand, an "opt-out" approach declares that a sender may send a message to a recipient even if there is no existing business relationship and the recipient has not specifically opted in to receiving the messages. Opt-out laws typically require senders to honor the requests of recipients to remove them from a sender's mailing list.[22] In other words, completely unsolicited messages may be sent; however, senders must stop their messages once they have been asked to do so. This basic approach was established by the first anti-spam law passed by the state of Nevada in 1997.[23] Today, approximately two-thirds of the world's anti-spam laws are considered opt-out, while approximately one-third are considered opt-in.[24]

Critics of opt-out laws charge that they "legalize spamming."[25] Because opt-out laws do not affirmatively establish that sending unsolicited e-mail is illegal, but instead provide a framework under which such messages may be sent, many anti-spam activists have suggested that they only make the problem worse.[26] On the other hand, critics of opt-in laws contend that they unreasonably burden legitimate businesses.[27] Direct marketers cite compelling statistics showing some e-mail users want to receive unsolicited offers via e-mail and closing that channel entirely is overly restrictive and burdensome.[28]

The debate over opt-in versus opt-out laws has been the subject of no less than 800 news articles, countless websites, and hours and hours of political discussion.[29] This rancor is in spite of the fact that the practical difference between opt-in and opt-out laws in terms of real enforcement is virtually nonexistent. If a spammer wishes to convert the strongest opt-in law into an opt-out law, all he or she needs to do is tell one lie: "The recipient requested to receive my messages."[30] While this may not be true, it forces a prosecutor to prove the negative—a task which is not only extremely expensive, but virtually impossible to accomplish definitively. Worse still, the spammer's statement may in fact be true. Studies have shown that online users regularly forget from which merchants they have opted in to receiving communication.[31] Users do not read privacy policies or the contracts that provide the extent to which a marketer may resell their personal information.[32] As a result, prosecutors face the risk under even opt-in regimes that their case may be scuttled by a forgetful end-user.

Empirically, the data on spam prosecutions proves the theory. While opt-in laws have proliferated in recent years, prosecutions under them are almost entirely nonexistent. In the United States, for example, the law which on paper appears to express the strongest sentiment against spam is Delaware's Law. In 1999, Delaware passed the world's first opt-in law regulating unsolicited commercial e-mail.[33] Like all opt-in laws that followed, Delaware's Law requires senders to receive a recipient's permission before sending commercial e-mail messages. If simply being opt-in were enough to allow easy prosecution, Delaware would be the leader among states in the United States convicting spammers. However, in the five years the state's law has been in effect there have been zero prosecutions. Around the world opt-in laws have met with a similar lack of any real enforcement.[34] While opt-in laws may express a strong and popular sentiment, to date they have done little to inspire any real action.

Somewhat surprisingly, two of the most effective anti-spam laws in the world belong to the states of Virginia and Washington in the United States. Both laws are, in fact, opt-out laws. Both appear relatively weak on paper. However, both laws were crafted to address the practical problems prosecutors face when enforcing laws against spammers. Virginia, for example, grants broad power to Electronic Mail Service Providers

(EMSPs) to enforce its law. As a result, much of the prosecutorial burden is transferred to private stakeholders. In this case, Virginia-based America Online (AOL) has used the law with substantial success when suing spammers. Virginia took advantage of the location of one of the world's largest EMSPs and transferred much of the prosecutorial burden to the private party. This is a successful strategy if the goal is to encourage as many effective prosecutions of spammers as possible. Unfortunately, it is a situation that is relatively unique to Virginia, as most jurisdictions do not host an EMSP with the clout or resources of AOL.

Washington state's anti-spam regime is interesting, creative, and more generally applicable. While the state's anti-spam law itself also appears particularly weak on paper,[35] the state prosecutor's office created a registry of e-mail addresses belonging to Washington residents.[36] This list is significant because it defines the addresses and individuals over which the state's jurisdiction extends. The effect of the registry is to put spammers on notice whenever they send to one of the registered addresses that they have subjected themselves to Washington's law. Establishing jurisdiction is one of the thorniest issues a prosecutor faces when enforcing an anti-spam law. This is not only true from state to state in the United States, but, on the international level, from country to country. Washington's action-oriented approach is clever in providing a mechanism to resolve this fundamental problem faced by prosecutors.[37] Again, the empirics prove the theory. In part because of its registry of addresses, government attorneys in Washington have become the only prosecutors in the United States to successfully sue a spammer living outside their own state's jurisdiction. To date, the state's attorney general has successfully prosecuted at least four spam cases to completion, more than any other government prosecutor worldwide.[38]

Finally, it is worth noting New York, another US state which has had some success suing spammers. Recently the state sentenced a notorious spammer to prison[39]—a distinction few other jurisdictions worldwide can claim.[40] Yet New York does not even have an anti-spam law on its books. Instead the state has relied on existing consumer protection and anti-fraud statutes when prosecuting spammers. Throughout the world, these action-oriented laws have been honed over time to assist prosecutors in trying difficult cases. In spite of what seems like a weak sentiment—usually simply that consumers should be protected from fraud—the laws address the legal challenges prosecutors face with action and have therefore been widely successful.[41] New York's consumer protection law, for example, provides strong investigation and subpoena powers to track down those individuals targeting the state's citizens with fraud.[42] There have been literally hundreds of prosecutions under New York's consumer protection law over the same six-year time period during which there have been practically none for all the world's anti-spam laws.[43]

The lesson is that the strength of the sentiment in the law bears little correlation to the successful enforcement of that law. Choosing an opt-in versus an opt-out approach is not what matters if your end goal is to stop spam. Either approach has the potential to be effective, but only if prosecutors are given adequate legal tools and resources to do their job. 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.

4 Understanding the prosecution of spammers

Prosecutors face a number of costs when bringing legal action against spammers. Understanding what these costs are, and how to minimize them, is critical to crafting effective anti-spam legislation. To begin, the costs of tracking down and identifying a spammer are substantial. Spammers use multiple techniques to hide their identities and make a prosecutor's job more difficult. The United States Federal Trade Commission recently described these costs as faced by two prosecutors:

> A prosecutor in Washington State spent four months and sent out 14 pre-suit civil investigative demands (CIDs) just to identify the spammer in one lawsuit. Likewise, in another case, it took the Virginia Attorney General, over the course of four months, multiple subpoenas to domain registrars, credit card companies, and Internet providers, and the execution of a search warrant, before having enough information to file a case against a spammer.[44]

These identification costs would actually be relatively minor if only a few cases needed to be filed. However, as cases against hundreds of spammers are likely needed before any real benefit or deterrence is achieved,

these costs quickly become prohibitive for an individual prosecutor. Remember also that Washington and Virginia have two of the most successful and well-crafted anti-spam laws in the world. The identification costs faced by prosecutors in other jurisdictions with less effective anti-spam laws are likely to be even higher.

In addition to the cost of tracking down spammers, prosecutors also face the costs of actually litigating a trial once a target has been identified. Under current laws in the United States, an Internet Service Provider who has sued numerous spammers estimates the litigation costs for such a prosecution start at US$ 100'000 and can quickly rise to nearly US$ 2 million if a spammer mounts an aggressive defense.[45] It should also be noted that the costs to government prosecutors are relative to the funds available to prosecute these cases. If a prosecutor has not been allocated a budget to bring anti-spam prosecutions in advance, then the costs are perceived even higher because they potentially offset monies that could be allocated to fight more serious crimes. Moreover, both the costs of identifying and prosecuting spammers must be factored by the likelihood of success a prosecutor has at trial. The less likely the prosecutor is to win a case, the higher the effective costs of identifying and prosecuting each spammer become.

Finally, any negative externalities borne by society as a result of prosecution must be included in the equation. For example, if legitimate businesses are overly burdened by a prosecutor's investigation of a spammer, then the cost to those legitimate businesses must be taken into account. All of the above costs are weighed against the benefits achieved as a result of a successful prosecution. These benefits include not only taking the spammer off the network, but also any fines that are ultimately collected from the spammer. Only if the overall benefits of bringing prosecutions against spammers outweigh their costs can we declare our anti-spam laws truly effective.

If these prosecutorial costs and factors were reduced to a mathematical formula, the effectiveness of anti-spam law could be expressed by the following conceptual equation:

$$\langle Effectiveness \rangle = B_{success} - \frac{C_{identfying} + C_{prosecuting}}{P_{success}} - C_{society}$$

The equation above expresses that the expected effectiveness of an anti-spam law is determined by a number of quantifiable factors. First, the effectiveness is proportional to the potential benefit to society from a single successful prosecution ($B_{success}$). Effectiveness is reduced by the costs of identifying ($C_{identifying}$) a spammer to be prosecuted and the costs of actually bringing the prosecution ($C_{prosecuting}$) against him or her. The impact of these costs is adjusted by the likelihood of success at trial ($P_{success}$). For example, if only half of trials brought are likely to be successful, then the net costs to achieve one success ($B_{success}$) is double the cost of identifying ($C_{identifying}$) and prosecuting ($C_{prosecuting}$) a single spammer. Finally, the overall effectiveness is reduced by any external costs to society that arise as a byproduct of prosecution ($C_{society}$).

Whether consciously or unconsciously, prosecutors inevitably run something similar to this equation before bringing a case. In order to justify prosecuting a spammer, the expected effectiveness quotient must be as high as possible. The problem with nearly all existing anti-spam laws is that when they are evaluated they typically result in a negative effectiveness quotient. If the effectiveness quotient is below zero, a rational prosecutor will never bring a case because the costs will inherently outweigh the benefits. Spammers too use a similar method to choose their behavior in light of existing anti-spam law. Under today's laws, they rightly conclude that the risk of prosecution is so low that they can continue their activity with impunity.

Scenario A:

$$1'000_{success} - \frac{100_{identfying} + 200_{prosecuting}}{0.20_{success}} - 50_{society}$$

Scenario B:

$$1'050_{success} - \frac{75_{identfying} + 175_{prosecuting}}{0.30_{success}} - 40_{society}$$

Figure 2. While it is difficult to predict precise prosecutorial costs and factors, imagine the two different hypothetical scenarios illustrated above. While the differences between scenario A and B appear minimal, scenario A evaluates to an expected effectiveness value of -550. In contrast, scenario B evaluates to an expected effectiveness value of approximately +177. Therefore, laws that favor scenario B are much more likely to be regularly enforced than scenario A. This is encouraging because it shows that small changes in prosecutorial costs and factors can result in significant changes in the expected effectiveness of an anti-spam law.

For an anti-spam law to be a successful deterrent to spammers, its expected effectiveness quotient needs to be increased. To do this, the next generation of anti-

spam laws must be action laws. Specifically, they must be drafted to either 1) increase the benefit from a successful prosecution ($B_{success}$), 2) decrease the cost of identifying a spammer ($C_{identifying}$), 3) decrease the cost of prosecution ($C_{prosecuting}$), 4) increase the probability of success at trial ($P_{success}$), or 5) decrease any external costs to society from investigating and bringing a trial ($C_{society}$). Ideally, the next generation of anti-spam laws will achieve all five of these goals.

5 Recommendations

It is time for governments around the world to try something new. The costs of enforcing existing anti-spam laws are too high and until we can effectively reduce them our laws will continue to provide no deterrent to spammers. We need to move away from sentiment laws and toward action laws. We need to pass laws that give prosecutors the tools and resources they need to effectively track down and prosecute spammers. While every legislature will need to adapt its own regulations to emphasize its law enforcers' strengths and overcome their particular weaknesses, below are five legislative suggestions which may prove fruitful going forward.

5.1 Create bright lines and increase perceived benefits

Where possible, lawmakers should strive to create the brightest lines possible under anti-spam laws. Ambiguities increase the costs not only to prosecutors, but also to innocent defendants who are wrongly hailed into court. The most effective anti-spam laws would be prosecuted without requiring the resolution of significant questions of fact. For example, a law making it illegal to send any messages containing or advertising pornographic materials to an e-mail address belonging to a school servicing minor children avoids a number of difficult legal issues. For one, under traditional anti-spam laws, prosecutors need to demonstrate that a recipient did not somehow "opt-in" to receiving the messages. However, under the hypothetical "Preventing Pornography in Schools Act," prosecutors would not need to prove whether messages received by a school's address were solicited or unsolicited. The mere fact that they were targeted to an e-mail address belonging to a school and accessible by children would be enough to constitute a crime. Prosecutors then would need only prove two things: 1) the messages contained pornography, and 2) they were targeted to an address belonging to a school servicing minor children. This sort of bright line reduces the costs and increases the likelihood of success at trial for a prosecutor. It therefore may significantly increase the expected effectiveness of the law.

In addition, today's spam problem has generally been characterized as a cost for businesses—creating losses in productivity and requiring investments in more hardware and filtering software.[46] These costs are significant, yet they have been generally characterized as a cost of doing business, and nothing more. Moreover, a single prosecution of a spammer is perceived as unlikely to do much of anything to reduce these costs. A prosecutor is thus unlikely to embark on a prosecution for fear of being perceived as wasting resources. To remedy this perception, legislators passing the next generation of anti-spam law should consider focusing on the worst parts of the spam problem instead of passing another omnibus statute. For example, studies have clearly indicated that two areas are the primary concern of e-mail users in regard to spam: pornography and fraud.[47] One recent study found that "[s]o extreme was the reaction [among e-mail users to unsolicited] pornography that eliminating it alone among all unsolicited electronic mail would go a long way toward softening spam's negative impact on Internet users".[48]

Somewhat counter-intuitively, focusing on one of these limited areas of the spam problem increases the perceived benefits and may allow prosecutors to more easily justify their enforcement efforts. For instance, a prosecutor in a particular jurisdiction could focus on spammers who send unsolicited pornographic material to children. Another jurisdiction could target spammers who use their messages to commit fraud aimed at seniors. Importantly, these focused laws and limited actions are less likely to impose negative external costs on legitimate businesses and more likely to be seen as a worthwhile use of prosecutorial resources. Maybe of equal importance, because of their focus these laws are less likely to be opposed and weakened by direct marketing lobbies. For prosecutors, the perceived benefit of this focused anti-spam law is increased and therefore overall effectiveness of the law is likely to rise. While such focused laws will not stop all spammers, it is more likely that if they are aggressively enforced, they will motivate many to change their current business model. Once the worst spammers have been removed from the network, legislatures can return to address the thornier problems of legitimate, non-objectionable companies using unsolicited e-mail to peddle their products.

5.2 Expand law enforcement tools and resources

Spammers are difficult to track down and law enforcers need as many tools and resources as possible to do so. Lawmakers should look first to their existing consumer protection statutes and replicate the investigatory and subpoena powers they create. They should also examine the evidentiary burdens their prosecutors are required to meet and determine whether there is any possible way to assist them when trying to make a case against a spammer.

One tangible example of a legislative tool that directly assists law enforcement in prosecuting spammers was passed as part of the United States' CAN-SPAM Act. While CAN-SPAM rightly deserves much criticism, one way in which the new law assists prosecutors is by allowing them to go after not only the actual spammer who presses the send button, but also the business that contracted with the spammer to advertise their products.[49] This vendor liability reduces the problem of tracking down a target substantially. In most cases, vendors have a significantly more difficult time than the actual spammer at hiding their identity or internalizing the costs from the risk of prosecution. If you can dry up the demand by vendors for spammers' services, eventually the problem of spam will be greatly diminished. Legislative tools that enable easier prosecution, such as the vendor liability provision from CAN-SPAM, should be considered for next-generation anti-spam laws.

Additionally, where possible, laws should be drafted in order to generate funds to aid in law enforcement. To start, any fines collected against spammers should be funneled back to the appropriate law enforcement agency in order to fund future prosecutions. Additional possibilities may exist. For instance, in the United States several states have passed "Do-Not-Call" statutes.[50] These measures establish lists of citizens who do not wish to be called by marketers. In order to receive access to a mechanism to scrub their internal calling lists of registered numbers, the do-not-call statutes require telemarketers to pay a fee to the state. In general, these fees have been used to fund the maintenance of the lists as well as any law enforcement efforts to prosecute violators of the law. Similar measures may be possible to create funding mechanisms for anti-spam enforcement efforts.

5.3 Share information internally and internationally

As prosecutors enforce more anti-spam cases, their expertise is likely to increase, and their average costs of identifying and prosecuting spammers are likely to decrease.[51] These costs can be more rapidly diminished if information is shared between multiple law enforcement agencies and across borders. Spammers hide themselves by exploiting the inefficiencies of cross-border cooperation and communications. In order to defeat these criminals, prosecutors from multiple jurisdictions should consider establishing a system in order to work together and exchange information. To some extent, ad hoc versions of these systems of cooperation are already beginning to emerge.[52] Encouragingly, South Korea and Australia recently signed a formal memorandum of understanding to share information on spam prosecutions.[53] These types of partnership are critical to defeat spam. Going forward, if information sharing mechanisms can be put in place between more countries, the knowledge of multiple jurisdictions can be shared and law enforcement efforts can be more effectively allocated. Such cooperation benefits every nation participating in the information society.

5.4 Enable more enforcers and investigators

It appears unlikely that governments alone will be able to mount the sustained effort needed to eliminate spammers. It makes sense, therefore, to enable other entities to enforce anti-spam laws. For example, as discussed above, Virginia has had substantial success allowing Internet Service Providers (ISPs) to enforce its law. Several commentators have argued that anti-spam laws will only be effective when individuals are allowed to enforce them.[54] In the United States, the problem of junk fax messages was proliferating in the early 1990s. The United States Congress responded by passing the Telephone Consumer Protection Act (TCPA) in 1996.[55] The law allowed individuals to sue senders for US$ 500 per unsolicited junk fax message received. While junk faxes have not been eliminated, since the passage of the law this problem has been greatly reduced.[56]

Expanding the right of individuals to sue is not without some risk. For example, in the state of Utah, an anti-spam law was passed that allowed a private right of action. The law was sloppily drafted, and encouraged even frivolous lawsuits.[57] Assuming the problems Utah experienced can be resolved with more careful drafting and fines for individuals who bring frivolous lawsuits, allowing more private enforcers shifts many

of the cost of identifying and prosecuting spammers away from the government. Lawmakers considering new anti-spam measures should contemplate widening the scope of those who are empowered to enforce the laws against spammers.

In addition, it may be possible for governments to encourage private citizens to do much of the tracking of spammers for them. Many private organizations are already dedicated to tracking down spammers. If these organizations and other enterprising individuals are rewarded with a small fee from governments they may, in effect, serve as private bounty hunters for prosecutors.[58] While it seems unlikely that such a system alone would be sufficient to deal with the spam problem, so long as negative impacts to society are minimized, and the fee paid to the bounty hunters is lower than the costs prosecutors would normally bear to identify spammers, such a programme may assist in creating an effective anti-spam regime.

5.5 Resolve jurisdictional ambiguities

Having interviewed prosecutors who have attempted to enforce current anti-spam laws, one of the foremost concerns they have is their ability to establish jurisdiction over a spammer. Most modern legal systems require that in order to be subject to the rules of a jurisdiction individuals must have "purposefully availed" themselves of that jurisdiction. The relative anonymity of an e-mail address means it is often unclear whether a spammer has met this standard. For example, if a British citizen receives spam at a Hotmail account with the e-mail address xyz@hotmail.com, whose jurisdiction applies? While the United Kingdom may have a vested interest in protecting its citizen from spam, courts worldwide are likely to hold that the only jurisdictions with the ability to prosecute the spammer are either Redmond, Washington where Microsoft, Hotmail's corporate parent, is based, or potentially Santa Clara, California, where Hotmail's servers are based.

The British citizen may be somewhat more likely to receive the protection of a court in the United Kingdom if the e-mail address in question is xyz@hotmail.co.uk—in other words if it uses a country-specific top level domain (TLD). However, legal precedent on this matter has not been established, and the answer is complicated by the fact that different countries have set different rules for issuing domains under their country-specific TLDs.[59]

Prosecutors need a clear and well-established mechanism to create a jurisdictional nexus between their citizens' e-mail addresses and their home jurisdiction. Spammers can then be considered on notice of what laws apply to which addresses and can be hailed into court accordingly. In order to do this, the Country Code Names Supporting Organization (ccNSO) should encourage countries controlling TLDs to modify their terms to include clear notice that addresses registered under them are subject to the laws of the controlling country.[60] In addition, jurisdictions should establish registries similar to the system created by Washington state. As was discussed above, the Washington registry has been upheld by courts in the United States as sufficient to create a legal basis through which a prosecutor may assert jurisdiction over a foreign spammer.[61] Until other governments create similar jurisdiction-enabling mechanisms they will continue to struggle with the ability to protect their citizens from spammers outside the natural reach of their laws.

6 Conclusion

Few people would dispute that around the world the first generation of anti-spam laws has been an unqualified failure. That, however, is not a reason to give up on law as a mechanism by which to combat spam. Instead, we need to focus on the tools prosecutors need to make anti-spam laws successful. The next generation must move beyond mere sentiment to real action. Where possible, these new laws must decrease the costs faced by prosecutors and increase their likelihood of success at trial. New laws must draw bright lines, resolve jurisdictional ambiguities, provide resources, and enable enforcement. While law alone is unlikely to completely rid the world of spam, it can make a substantial and unique contribution. However, this contribution is only possible if we move beyond the mistakes we have already made, and proceed to a new class of laws designed from the beginning to actually do some good.

T[1] *See* David E. Sorkin, *Spam Laws* <http://www.spamlaws.com/> (accessed 12 June 2004). *See also* Direct Marketing Association, *Executive Summary of International Spam Laws* <http://www.the-dma.org/antispam/spamlaws.html> (accessed 12 June 2004).

2 *See* Nev. Rev. Stat. §§ 41.705–735, 1997.

3 *See* David E. Sorkin, *Spam Laws* <http://www.spamlaws.com/> (accessed 12 June 2004). *See also* Direct Marketing Association, *Executive Summary of International Spam Laws* <http://www.the-dma.org/antispam/spamlaws.html> (accessed 12 June 2004).

4 *See* Lorrie Faith Cranor and Brian A. LaMacchia, *Spam!*, 41 Communs. of the ACM 8, 76, Aug. 1998.

5 *See* InsightExpress/Unspam, 2003 *Comprehensive Spam Survey*, 12 Oct. 2003 <http://www.unspam.com/fight_spam/information/survey_personal.html> (accessed 10 June 2004).

6 *See* InsightExpress/Unspam Survey cited in note 4.

7 *See* 15 USC. § 7705. CAN-SPAM stands for the "Controlling the Assault of Non-Solicited Pornography and Aggressive Marketing." It was signed into law 16 Dec. 2003 and became effective 1 Jan. 2004.

8 *See* David McGuire, *Report: More Spam Violates Law*, Washington Post, 9 June 2004 <http://www.washingtonpost.com/wp-dyn/articles/A29136-2004Jun9.html> (accessed 17 June 2004) (citing study by anti-spam vendor MX Logic).

9 *See* McGuire article cited in note 7.

10 In 1997, e-mail filtering was generally limited to individual regular expressions through programs such as Procmail. SpamAssassin, the widely used open-source anti-spam filter, was first conceived in 1998 and only released to the public in 2001. *See SpamAssassin PreHistory* <http://spamassassin.org/prehistory/> (updated 14 July 2003); *SpamAssassin History* <http://wiki.spamassassin.org/w/SpamAssassinHistory> (updated 9 Dec. 2003). Brightmail, a leading anti-spam filtering company, was a leader in this space, having been founded in 1998. *See Brightmail — Company* <http://www.brightmail.com/about_us.html> (accessed 14 June 2004). The general point is that spam filtering has emerged at the same time as the dramatic increase in the volume of spam.

11 *See* Rebecca Lieb, *FTC Spam Forum*, (FTC Conf. Cent., Washington, DC, 1 May 2003) (a discussion of the economics of spam, and the low barrier to entry into the spam business); *see also* Bill Gates, *On Spam: Wasting Time On the Internet*, Microsoft Corporation, 25 Mar. 1998 <http://microsoft.com/billgates/columns/1998Essay/3-25col.asp> (accessed 17 June 2004) ("The incremental cost of sending a message on the Internet is essentially zero. This has wonderful implications. Unfortunately, it has led to junk mail being sent to tens of thousands of people — wasting an enormous amount of their collective time — at almost no cost to the senders.").

12 *See* Rebecca Lieb, *FTC Spam Forum*, FTC Conf. Cent., Washington, DC, 1 May 2003.

13 Estimates vary as to how many spammers are operating worldwide. However, the consensus appears to be that there are around 200 "kingpin" spammers responsible for the vast majority of the spam problem. *See, e.g.*, Robert Wientzen, *FTC Spam Forum*, FTC Conf. Cent., Washington, DC, 30 Apr. 2003, (likely 200 spammers responsible for at least 80 per cent of the problem); *see also* Spamhaus Project, *Register of Known Spam Operations* <http://www.spamhaus.org/rokso/> (accessed 12 June 2004) (approximately 200 spam organizations, and between 500–600 individuals, responsible for 90% of the spam problem).

14 This is a bit of a simplification. In fact, the rate at which spam is fed to our inboxes is a function of a variety of costs. Below is a more accurate accounting of how costs from multiple sources would impact this spam rate:

$$\frac{d(spam)}{dt} = (k1 \times B_{sendingspam} - k2 \times C_{technical} - k3 \times C_{legal} - k4 \times C_{social})$$

Spammers receive a certain benefit from sending spam (their profit) and will increase their spam output proportional to this profit. This benefit is offset by the technical costs of sending spam (bandwidth, computer equipment, etc), legal costs (the risks of fines, jail time, etc), and finally social costs (being shunned by friends, living as an outlaw, etc). As a result, any effort to increase costs ,while maintaining or decreasing the benefit spammers receive, will reduce the overall rate of spamming .

[15] Several analysts have suggested that e-postage is the only way to control spam. *See, e.g.*, Eric Allman, *The Economics of Spam*, Queue, Dec. 2003–Jan. 2004 <http://acmqueue.org/modules.php?name=Content&pa=showpage&pid=108> (accessed 18 June 2004) (co-founder of Sendmail argues increasing the cost to senders is the solution to the spam problem); *see also* Jim Nail, *The Real Answer to the Spam Problem*, Forrester Research, 10 Dec. 2003 <http://www.forrester.com/ER/Research/Brief/Excerpt/0,1317,33324,00.html> (accessed 17 June 2004) ("The only permanent solution to the spam problem is to charge for email"). Microsoft and other companies are investigating mechanisms to implement such an e-postage scheme. *See, e.g.*, Associated Press, *Gates: Buy Stamps to Send E-Mail*, CNN, 5 Mar. 2004 <http://www.cnn.com/2004/TECH/internet/03/05/spam.charge.ap/> (accessed 12 June 2004) (Microsoft's "Penny Black" project would create e-postage for e-mail messages).

[16] Even the most successful anti-spam laws, such as the laws in the states of Virginia and Washington in the United States, have only been enforced a handful of times.

[17] *See* Graham Hughes, *The Crime of Incest*, 55 J. Crim. L. & Criminology 322, 329-30, 1964.

[18] *See, e.g.*, Australian Criminal Code Act of 1995, sec. 101, et. seq. (allows prosecution for preparation of terrorist activities); French Anti-Terrorism Act of 2001 (expand the abilities of police to conduct searches); India Provention of Terrorism Act of 2001 (allows special police powers to combat terrorism); Japan Anti-Terror Special Measures of 2001 (special provisions to share information with the International community); Northern Ireland (Emergency Provisions) Act, 1987, c. 30, 14(1) (allows sweeping measures to combat terrorism); United Kingdom Anti-Terrorism, Crime and Security Act 2001, Ch. 24 (allows the seizure of terrorist funds, creates special agency to combat terrorism); United States Patriot Act of 2001 & United States Homeland Security Act of 2002 (expand police powers to investigate terrorism, creates special departments within the government to investigate terrorist activities). It should be noted that these laws have not come without criticism. The public's interest must always be weighed when allowing the police to have special powers so as to ensure that civil liberties are not sacrificed.

[19] *See, e.g., Interview with Peter Lejeune, Senior Associate, Security Management International, Inc*., 6 Geo. Public Pol'y Rev. 125, Spring 2001 (discussing how laws that simply express sentiment do little to deter terrorists).

[20] *See, e.g.*, laws cited in note 17; *see also* Lejeune interview cited in note 18.

[21] For example, under the European Union's Directive 2002/58/EC, Art. 13, para 2 allows unsolicited e-mail to be sent if an address was obtained in connection with sale of product or service, and a customer is allowed to opt-out of future mailings.

[22] For example, under the United States CAN-SPAM Act, 15 USC. § 7705, Sec. 5(a)(3), requires marketers provide a mechanism whereby recipients can request to no longer receive messages from a sender.

[23] Interestingly, Nevada's law was first drafted to create an "opt-in" regime. The original bill that gave rise to the Nevada statute, SB-13, was sponsored by Republican Senate Majority Leader William Raggio. *See Nevadans Against Spam*, CNET News.com, 20 Jan. 1997 <http://news.com.com/2100-1023-263458.html> (accessed 10 June 2004). As the bill progressed through the Nevada legislature, it was amended under pressure from direct marketers to instead create the weaker "opt-out" standard. *Id.*

[24] A majority of the 37 anti-spam laws passed by states in the United States have been some form of an opt-out law. *See* David E. Sorkin, *Spam Laws* <http://www.spamlaws.com> (accessed 12 June 2004). The Federal CAN-SPAM Act in the United States also is an opt-out law. *Id.* On the other hand, the European Union has directed its member states to pass opt-in laws. *Id.* Most anti-spam laws passed prior to 2002 were opt-out laws. With these first opt-out laws having little effect to curb spam, it appears the trend in the last two years has generally been toward opt-in laws. *Id.*

[25] *See* Spamhaus Project, *United States Set to Legalize Spamming January 1, 2004*, 22 Oct. 2003 <http://www.spamhaus.org/news.lasso?article=150> (accessed 14 June 2004) (CAN-SPAM, the opt-out law passed by the United States Congress, was roundly criticized).

[26] Critics have suggested that opt-out laws give a legal framework under which unsolicited commercial e-mail may legally be sent. As a result, many believe that they may actually make the problem worse. *See, e.g.*, Dinah Greek, *New Laws Will Make Spam Worse*, Vnunet.com, 9 Jan. 2004 <http://www.vnunet.com/news/1151902> (accessed 13 June 2004).

[27] *See, e.g.*, Fred H. Cate and Michael E. Staten, Prot*ecting Privacy in the New Millennium: The Fallacy of "Opt-In,"* Direct Marketing Association <http://www.the-dma.org/isec/optin.shtml> (accessed 16 June 2004).

[28] *See, e.g.*, Peter A. Johnson, *Preserving the Promise of the E-Mail Marketplace*, Direct Marketing Association, 31 Mar. 2004 (a significant number of consumers want to receive offers via e-mail).

[29] A search of the Lexis-Nexis English news archive for "opt-in /p opt-out & (spam OR unsolicited) & (law OR legislation)" finds 921 articles published since 2000. In terms of websites, a search of Google for "opt-in opt-out (spam OR unsolicited) (law OR legislation)" finds 61'700 pages.

[30] This is a regular defence of spammers which a survey of anti-spam complaints filed to date shows is raised at nearly every trial. Regardless of whether it is true, it expends a prosecutor's time and resources attempting to prove it is not.

[31] Studies by direct marketers in the United States have found that at least 5% of all individuals who opt-in to a mailing list will forget they have done so within 30 days. *See* Marketing Sherpa, *Spam & Privacy Information for Marketers* <http://www.marketingsherpa.com/sample.cfm?contentID=1620> (updated 24 Apr. 2001). As time passes, memory and evidence for what individuals actually have opted-in to fades quickly. This presents a real problem for law enforcers.

[32] As few as 3% of online users read the privacy policies that disclose how companies may use their personal information. *See* Harris Interactive, *Privacy Notices Research: Study No. 15338*, Dec. 2001. As a result, many users may be agreeing to allow marketers to target them with advertisements without realizing. This again presents a substantial problem for law enforcers.

[33] *See* Del. Code Ann. tit. 11 §§ 931, 947–48, 1999.

[34] Because prosecutors even under opt-in regimes have generally not been granted the tools needed to enforce the laws, there have been virtually no prosecutions. *See, e.g.*, Graeme Wearden, *UK Spammers Set to Avoid Prosecution Until 2005*, ZDNet UK, 16 Apr. 2004 <http://news.zdnet.co.uk/business/legal/0,39020651,39152267,00.htm> (accessed 18 June 2004).

[35] *See* Wash. Rev. Code §§ 19.190.005–19.190.050, 1998. In relevant part, the Washington anti-spam law requires "no misleading subject lines" and "no forged header or routing information." This appears comparatively weak compared with not only European opt-in laws, but also other United States anti-spam laws which have proven less enforceable.

[36] The registry of Washington-based e-mail addresses is available online at: http://registry.waisp.org.

[37] A United States court evaluating the jurisdiction issue has determined that the Washington registry is sufficient to put spammers on notice of which addresses belong to the state's residents. *See State v. Heckel*, 24 P.3d 404, Wa. Sup. Ct. 2001. As a result, spammers who send to an address on the registry are seen as having purposefully availed themselves of the state's jurisdiction and can be hailed into Washington's courts to be prosecuted. *Id*.

[38] *See* Paula Selis, *FTC Spam Forum*, FTC Conf. Cent., Washington, DC, 2 May 2003.

[39] *See* Reuters, *"Buffalo Spammer" Sent to the Slammer*, Wired News, 27 May 2004 <http://www.wired.com/news/technology/0,1282,63640,00.html> (accessed 14 June 2004) (prolific New York-based spammer was sentenced to prison for consumer fraud).

[40] A handful of criminals who used spam as part of their schemes to defraud have been sentenced to jail. For example, in the United States the Department of Justice successfully prosecuted Zachary Keith Hill for "orchestrating a scheme to defraud consumers of personal financial information via spam email," K.C. Smith for using spam to further a securities fraud scheme, and Steve Shklovskly and Yan Shtok for using spam to promote a fraudulent employment scheme. *See* US Dept. of Justice Press Release, *Fraudster Sentenced to Nearly Four Years in Prison in Internet 'Phishing' Case*, 18 May 2004 (Hill sentenced to 46 months in prison); US Dept. of Justice Press Release, *Operation 'Cyber-Sweep' Targets Online Fraud*, 20 Nov. 2003 (Smith sentenced to 14 months in prison); James Evans, InfoWorld, *Two Sentenced in Major E-Mail Spam Scam*, 22 Jan. 2001 (the pair sentenced to 27 months in jail). A Welsh court sentenced Peter Okoeguale, a so-called "Nigerian spammer," to 20 months in prison for an advanced fee fraud scam. *See* Western Mail, *Man Jailed for Email Scam*, 3 Apr. 2004. An Australian court sentenced Steven Hourmouzis to two years in jail for using spam as part of a stock "pump and dump" scheme. *See* Eli Greenblat, The Age, *ASIC Wins Guilty Plea In Internet Spam Scam*, 8 Mar. 2001. The first arrests of individuals for merely sending spam took place in Virginia in December of last year. *See* Software World, *Suspected Spam Lord Charged*, 1 Jan. 2004. The Virginia case is still pending.

41 In the United States, consumer protection statutes have generally been drafted so as to be as easy to enforce as possible in order to empower consumers to control abuse by fraudulent businesses. *See, e.g., Consumer Action Website* <http://consumeraction.gov/> (accessed 17 June 2004). It appears similar motivations have been cited by governments worldwide when passing consumer protection statutes.

42 *See, e.g.*, NY CLS Gen Bus § 349, et. seq., 2004 (granting broad subpoena powers to the state's attorney general); NY CLS Exec § 550, et. seq., 2004 (constituting a special consumer protection board to investigate complaints).

43 Information on successful prosecutions under consumer protection laws in New York state is available online at: http://www.oag.state.ny.us/. Again, the important point is that a single jurisdiction has been able to prolifically enforce consumer protection laws drafted to aid in enforcement, while the rest of the world has been almost completely unable to enforce its sentiment-based anti-spam laws.

44 *See* Federal Trade Commission, *National Do-Not-Email Report to Congress*, 15 June 2004 <http://www.ftc.gov/reports/dneregistry/report.pdf> (accessed 16 June 2004).

45 *See* Federal Trade Commission report cited in note 43.

46 *See, e.g.*, Jay Lyman, Spam Costs US$ 20 Billion Each Year in Lost Productivity, TechNewsWorld, 29 Dec. 2003 <http://www.technewsworld.com/perl/story/32478.html> (citing a Basex study estimating annual cost of spam at US$ 20 billion to US-based businesses); Paul Roberts, Report: Spam Costs US$ 874 Per Employee Per Year, InfoWorld, 1 July 2003 <http://www.infoworld.com/article/03/07/01/HNspamcost_1.html> (citing Nucleus Research study finding spam costs the average company US$ 874 annually); Associated Press, Study: Spam Costs Businesses US$ 13 Billion, CNN.com, 5 Jan. 2003 <http://www.cnn.com/2003/TECH/biztech/01/03/spam.costs.ap/> (citing Ferris Research study finding cost of spam to US businesses is US$ 8.9 billion annually).

47 *See* Deborah Fallows, *Spam: How it is hurting e-mail and degrading life on the Internet*, *Pew Internet & American Life Project*, 22 Oct. 2003 <http://www.pewinternet.org/reports/toc.asp?Report=102> (accessed 8 June 2004); *see also* Center for Policy and Leadership, University of Illinois at Springfield, *Statewide Survey of Spam and Internet Sales Tax*, 17 June 2004.

48 *See* Fallows report cited in note 46.

49 *See* 15 USC. § 7705, Sec. 6. This section of CAN-SPAM specifies:

> (a) IN GENERAL — It is unlawful for a person to promote, or allow the promotion of, that person's trade or business, or goods, products, property, or services sold, offered for sale, leased or offered for lease, or otherwise made available through that trade or business, in a commercial electronic mail message the transmission of which is in violation [...] if that person —
>
> (1) knows, or should have known in the ordinary course of that person's trade or business, that the goods, products, property, or services sold, offered for sale, leased or offered for lease, or otherwise made available through that trade or business were being promoted in such a message;
>
> (2) received or expected to receive an economic benefit from such promotion; and
>
> (3) took no reasonable action —
>
> (A) to prevent the transmission; or
>
> (B) to detect the transmission and report it to the [Federal Trade Commission].

50 Forty-two states, as well as the Federal Trade Commission, have implemented do-not-call laws. These laws have generally been seen as extremely successful. *See Gryphon Networks: Latest DoNot-Call News and Regulatory Information*, Summer 2004 <http://www.gryphonnetworks.com/press/newsletters/2003_06/2003_06.html> (accessed 10 June 2004) (at least US$ 4'618'150 in fines as of June 2004). In addition to the fines, states generally require a fee of approximately US$ 1'000 to be paid by telemarketers in order to access the state's do-not-call registry. These fees are generally directed toward enforcement and administration of do-not-call laws.

51 The relationship between enforcement and costs can be described more formally by following the rate of accumulation of prosecution-relevant information as a function of time:

$$\frac{dI}{dt} = \left(\sum_{i}^{N} S_i \right) - k_d I + k_{legal} N_{legal\ \ successess}$$

Here I is the amount of prosecution related information, S_i is a source of information, M is the number of sources, and N is the number of legal successes. In this expression, sources and legal successes provide information, while useful information is lost because it is outdated (k_d). From this expression, we can conclude that if the information learned from each legal success can be shared with other law enforcers, then the benefit of each success is significantly increased across the entire network.

[52] The Spamhaus Project, for example, works with law enforcement agencies to help them identify spammers. For more information visit their website: http://www.spamhaus.org/. What is needed in addition to efforts such as these is a backchannel through which law enforcement agencies can communicate and exchange data on spammers and other cyber criminals. Interpol reportedly has some systems in place to combat more serious cyber crimes; however, some law enforcers have suggested they are currently not set up to deal with the problem of spam. In order to receive international cooperation, it may be necessary to initially focus on a limited, and particularly troublesome, aspect of the spam problem about which virtually all countries can easily agree (*e.g.*, pornographic content targeting children, identity theft scams, etc.).

[53] *See* Australian Communications Authority, *Australia and Korea sign spam MoU*, 20 Oct. 2003 <http://www.aca.gov.au/aca_home/media_releases/media_enquiries/2003/03-40.htm> (accessed 21 Jun 2003).

[54] *See, e.g.*, David Kramer, *FTC Spam Forum*, FTC Conf. Cent., Washington, DC, 1 May 2003. *See also* Tim Lemke, *New Law Bans Spam, Allows For Suits Against Senders*, 24 Sept. 2003 <http://www.washtimes.com/business/20030923-111201-2803r.htm> (accessed 21 June 2004).

[55] *See* 47 USC. 227, 1996.

[56] *See* Kramer discussion cited in note 53 (TCPA has made a significant dent in the amount of unsolicited fax messages sent since 1991).

[57] *See* Kramer discussion cited in note 53. *See also* Bob Mims, *Spam Filings Flood Court*, 18 July 2003 <http://www.sltrib.com/2003/Jul/07182003/utah/76385.asp> (accessed 21 June 2004).

[58] This bounty hunting proposal was originally suggested by Lawrence Lessig, a Stanford University law professor. *See* Lawrence Lessig, *Code Breaking: A Bounty on Spammers*, CIO Insight, 16 Sept. 2002 <http://www.cioinsight.com/article2/0,1397,1454839,00.asp> (accessed 19 June 2004). Lessig literally bet his job that his proposal would be successful. The proposal was mentioned in CAN-SPAM and the Federal Trade Commission is currently considering its merits. *See* 15 USC. § 7705, Sec. 11.

[59] Rules for various country TDLs vary widely from country to country. For example, some only allow individuals within the country to register domains (*e.g.,* Canada .CA, Mongolia .MN). Others allow anyone willing to pay the fee to register a domain within the TLD (*e.g.,* Armenia .AM, Austria .AT, Cocos Islands .CC, Niue .NU, Samoa .WS, Tonga .TO, Turkmenistan .TM, and Tuvalu .TV).

[60] The Country Code Names Supporting Organization (ccNSO) is a division of the International Corporation for Assigned Names and Numbers (ICANN). For more information visit ccNSO's website at http://ccnso.icann.org/.

[61] *See Heckel* case discussed in note 36. *See also Ferguson v. Friendfinders*, 94 Cal. App.4th 1255, 1265, Ca. App. 1st Dist. 2002 (holding a spam law may apply to a foreign spammer if there is a mechanism in place for the spammer to determine which addresses belong to a particular jurisdiction's residents).