INTERNATIONAL TELECOMMUNICATION UNION

WSIS Thematic Meeting on Cybersecurity

Geneva, 28 June – 1 July 2005

Document: CYB/03 Prov.
10 June 2005

DRAFT

A COMPARATIVE ANALYSIS OF SPAM LAWS: THE QUEST FOR A MODEL LAW

June 2005

The paper was prepared by Derek E. Bambauer, John G. Palfrey, Jr., and David E. Abrams, Berkman Center for Internet & Society Harvard Law School, for the ITU WSIS Thematic Meeting on Cybersecurity.

Notes on the Authors

David E. Abrams – David Abrams holds a J.D. from Harvard Law School and a B.S.E.E. and an M.S.E.E from the Massachusetts Institute of Technology. David designed analog and digital instrumentation for Thornton Associates, Digilab and Natural Microsystems before co-founding Galactic Industries Corp, a scientific software company (since acquired by a division of Thermo Electron). His research interests include spam, intellectual property, internet technology and First Amendment issues. David will be joining Wilmer Cutler Pickering Hale and Dorr in Boston as an Intellectual Property Associate in the fall of 2005.

Derek E. Bambauer – Derek Bambauer is a Research Fellow at the Berkman Center for Internet & Society at Harvard Law School. He holds a J.D. from Harvard Law School and a B.A. from Harvard College. Derek spent five years working for Lotus Development Corp. (now a division of IBM) as a principal systems engineer, Web developer, and technical writer. Among his specialties were Internet messaging, server architecture, and data recovery. His research interests include spam, Internet filtering and censorship, intellectual property, spyware, and cognitive effects on human decisionmaking.

John G. Palfrey, Jr. – John Palfrey is Executive Director of the Berkman Center for Internet & Society and Lecturer on Law at Harvard Law School. John works with the Center's co-directors to set and carry out the Center's ambitious, public-spirited agenda and oversees the work of its staff, fellows and students. John teaches courses on Internet law, e-commerce, and digital democracy. He is a lead researcher on the Digital Media Project, which studies the transition from analog to digital entertainment, and the OpenNet Initiative, a collaborative project with the Universities of Cambridge and Toronto to example the way that countries block their citizens' access to the Internet. Along with Professors Jonathan Zittrain and William Fisher, he co-authored an amicus brief to the U.S. Supreme Court in *MGM v. Grokster*. He has published a number of scholarly papers related to the Internet's relationship to Intellectual Property, international governance, and democracy. He writes a blog at http://blogs.law.harvard.edu/palfrey/. Prior to joining the Berkman Center, he practiced intellectual property and corporate law at the law firm of Ropes & Gray. John worked as a White House-appointed special assistant at the U.S. Environmental Protection Agency during the Clinton Administration. He is a former founder and officer of a venture-backed software company. He is a graduate of Harvard College, the University of Cambridge, and Harvard Law School.

A COMPARATIVE ANALYSIS OF SPAM LAWS: THE QUEST FOR MODEL LAW

Executive Summary

Spam presents a significant challenge to users, Internet service providers, states, and legal systems worldwide. The costs of spam are significant and growing, and the increasing volume of spam threatens to destroy the utility ofelectronic mail communications.

The Chairman's Report from the ITU WSIS Thematic Meeting on Countering
Spam in July 2004 emphasized the importance of a multi-faceted approach to solving the problem of spam and named legal governance as one of the necessary means. Our paper focuses on the potential nature of the legal regulation of spam, specifically the importance of harmonizing regulations in the form of a model spam law. We agree with the Chairman that the law is only one means towards this end and we urge regulators to incorporate other modes of control into their efforts, including technical methods, market-based means, and norm-based modalities.

Spam uniquely challenges regulation because it easily transverses borders. The sender of a message, the server that transmits it, and the recipient who reads it may be located in three different states, all of which are under unique legal governance. If spam laws are not aligned
in these states, enforcement will suffer because the very differences between spam laws may mean that a violation in one state is a permissible action in another. Moreover, spammers have an incentive to locate operations in places with less regulation, and the opportunity to states to create a domestic spam hosting market may engage them in a race to the bottom.

Harmonizing laws that regulate spam offers considerable benefits, insofar as a model law could assist in establishing a framework for cross-border enforcement collaboration. To those enforcing the regulation of spam, harmonization as a model law effort offers: clear guidelines, easy adoption, enhanced enforcement, stronger norms, fewer havens for spammers, and the increased sharing of best practices. If such regulators then agree that harmonization can aid legal regimes intent on curbing spam, they must initially address four critical tasks: defining prohibited content, setting default rules for contacting recipients, harmonizing existing laws, and enforcing such rules effectively. This legal approach must be concurrently matched by efforts that employ other modes of regulation, such as technical measures, user education, and market-based approaches.

Our analysis of existing spam legislation gathered by the ITU Strategy and Policy Unit evaluated these laws' elements to determine whether they were commonly included or not, and whether provisions were uniformly implemented or varying when present. Our research documents seven instances in which extant laws strongly converge: a focus on commercial content, the mandatory disclosure of sender/advertiser/routing, bans on fraudulent or misleading content, bans on automated collection or generation of recipient addresses, the permission to contact recipients where there is an existing relationship, the requirement to allow recipients to refuse future messages, and a mix of graduated civil and criminal liability. Also documented are five key areas of disagreement which are vital to a harmonized spam law but which have evaded consensus thus far: a prior consent requirement for contacting recipients, a designated enforcer, label requirements for spam messages, the definition of spam (whether it is limited to e-mail communication, or includes other applications, such as SMS), and the jurisdictional reach of the system's spam laws. Naturally, a harmonization effort must tackle and narrow these zones of divergence in order to succeed.

Spam laws, whether harmonized or not, are at best only part of the solution to the spam problem and must be developed in concert with technical, market, and norms-based tools if the scourge of spam is to be substantially reduced. Efforts to harmonize the legal regulation of spam can serve as one effective means

to solving the unique challenges spam presents. A model spam law is possible to develop, despite the many differences among the world's spam laws.

Table of Contents

I. Introduction 7
A. Purpose, Scope, and Methods 7
B. The Spam Problem 7
C. Attempts at Control 8
D. Evaluating Model Spam Legislation 9
II. Key Factors in Regulating Spam Through Legislation 11
A. Defining Prohibited Content 11
B. Setting Default Rules for Contacting Recipients 12
C. Harmonizing Existing Laws 12
D. Enforcing Rules 13
E. The Limits of Law, and The Need for Other Modes of Regulation 14
III. A Typology of Existing Spam Laws 15
A. Introduction 15
B. Defining Prohibited Content 16
C. Setting Default Rules for Contacting Recipients 18
D. Harmonizing Existing Laws 24
E. Enforcing Rules 25
F. Points of Convergence / Consensus 32
G. Points of Divergence / Difference 33
H. Conclusion 33
IV. Other Modes of Control: Potential Dependencies for Spam Laws 34
A. Technical Measures 34
B. Enforcement Efforts 40
C. User Education 40
V. Initial Recommendations 42
A. Defining Prohibited Content 42
B. Setting Default Rules for Contacting Recipients 42
C. Harmonizing Existing Laws 43
D. Enforcing Rules 43
VI. Conclusion 45

I. Introduction

A. Purpose, Scope, and Methods

The goal of this paper is to help policymakers understand the potential benefits and challenges of model spam legislation as a tool to improve the security of and user confidence in information and communications technology (ICT), as well as the potential that model spam legislation holds for Internet users worldwide.[1] First, it sets forth a framework for understanding spam and identifies key issues confronting regulators. Next, the paper examines the set of options for spam laws based on existing and proposed legislation gathered by the International Telecommunication Union (ITU) Strategy and Policy Unit (SPU).[2] It analyzes the level of consensus among these extant laws and the degree to which a particular component is included in most legislation and in the degree to which provisions addressing this component are similar or harmonized. The paper points towards zones where there is considerable consensus while simultaneously illuminating the most fundamental differences, so that policymakers can tackle the hard issues and choices involved in spam laws. Finally, the paper makes preliminary recommendations for spam law efforts and considers both the potential for and the likely efficacy of a model spam law.

The paper's scope is limited to analyzing the potential for the harmonization of spam laws, the key issues facing an effort to align regulation, and the zones of consensus and disagreement in existing legislation. We have not drafted a model law, but rather have framed and categorized the issues that drafters would need to take up. Moreover, the paper necessarily elides other important aspects of the fight against spam, including technical efforts to alter the underlying protocols that make electronic communication possible and the educational moves to instill a healthy skepticism in Internet users regarding spam. Our task is to frame the challenges and benefits of a model spam law and to provide initial suggestions on how one might undertake such an effort.

The methods involved in developing this paper include legal analysis of the legislation collected by the SPU and technical analysis of Internet messaging and spam analysis.

We conclude that a model spam law is possible to develop, despite the many differences among the world's spam laws. Such a model law could help in the efforts to combat spam, insofar as a model law could assist in establishing a framework for cross-border enforcement collaboration. Spam laws, whether harmonized or not, are at best only part of the solution to the spam problem and must be developed in concert with technical, market, and norms-based approaches if spam is to be substantially reduced.

B. The Spam Problem

Spam presents a significant challenge to users, Internet service providers, states, and legal systems worldwide. The costs of spam are significant and growing, and message volume threatens to destroy the utility of electronic mail communication. Postini, Inc., a provider of e-mail security services for corporations, reported that only 12% of the seven billion messages it processed in November 2004 was legitimate e-mail.[3] Estimates of the worldwide cost of spam to consumers and businesses reach as high as

[1] *See* §§ 35-37, *World Summit on the Information Society: Declaration of Principles*, Dec. 12, 2003, *available at* http://www.itu.int/wsis/documents/doc_multi-en-1161|1160.asp.
[2] *See* International Telecommunication Union, *ITU Activities on Countering Spam*, *at* http://www.itu.int/osg/spu/spam/law.html.
[3] Hiawatha Bray, *Frontier Justice Won't Stop the Spam*, BOSTON GLOBE, Dec. 6, 2004, at C3.

$20 billion each year.[4] These costs include: time spent deleting unwanted messages; the cost of software, hardware and services designed to block unwanted spam; the cost of bandwidth to handle transmission; and the costs for server storage and processing required to deal with the unwanted messages.[5] In addition, there are intangible costs: legitimate messages that are erroneously filtered by spam blocking systems; loss of efficiency as users turn to less useful communications mechanisms when e-mail becomes unreliable; and the harm to Internet domain owners' reputations whose domains are spoofed in fraudulent e-mail.[6] Finally, a significant percentage of spam promotes some type of fraud against the recipient, including viruses which infect the recipient's computer to gain control over it or to return proprietary information, phishing attacks[7] (which attempt to trick users into revealing financial passwords or PIN numbers), illegal financial schemes, and offers for products of dubious quality or legality.[8]

The impact of spam on individual users and their employers is considerable. According to a study prepared by Rockbridge Associates, seventy-eight percent of adults in the United States receive at least one unsolicited bulk e-mail message each day, with more than one-third receiving more than ten spam e-mail messages per day and eleven percent receiving more than forty unsolicited messages a day.[9] A 2003 study estimated that the average business employee receives 13.3 spam messages daily.[10]

Moreover, the spam problem grows at a rapid rate. One newspaper article notes that junk e-mail made up only 7% of e-mail traffic in 2001, but more than fifty percent in 2003.[11] A recent *New York Times* story estimated current junk mail traffic at eighty percent of all Internet electronic mail bandwidth.[12] In short, the flood of unwanted, often fraudulent messages known as spam creates a regulatory challenge that is sizeable, growing, and important. Spam also adapts to each major new technological advance, from e-mail to mobile phones to blogs and Really Simple Syndication (RSS) feeds.

C. Attempts at Control

Responses to spam's challenges have been attempted on a variety of fronts, including technical measures (such as filtering out messages identified as spam), educational moves (such as encouraging users not to

---

[4] *Id.*; *see also* Anick Jesdanun, *Deleting Spam Costs Billions, Study Finds*, SILICONVALLEY.COM, Feb. 2, 2005, *at* http://www.siliconvalley.com/mld/siliconvalley/news/editorial/10800628.htm (citing a Rockbridge Associates and University of Maryland study estimating the loss in productivity from spam to U.S. businesses at $21.6 billion).

[5] Bandwidth refers to the capacity, usually measured in quantity of electronic data per unit of time, that a digital communications channel can support. It is analogous to the size of the pipes used to deliver water or gas. A higher volume of electronic traffic requires higher bandwidth, just as a higher volume of water requires larger pipes. *See* Answers.com, *Bandwidth*, *at* http://www.answers.com/bandwidth (last visited June 7, 2005).

[6] Spoofing occurs when the sender of an e-mail message uses the return e-mail address of a third-party person or organization without permission so it appears that the e-mail comes from the third party. Because of the design of the Internet e-mail system, spoofing is extremely easy to accomplish.

[7] *See generally* Anti-Phishing Working Group, *at* http://www.antiphishing.org/index.html (describing types of phishing attacks and the existence of an organization of commercial and law enforcement interests focused on eliminating it) (last visited June 7, 2005).

[8] *See* United States Federal Trade Commission, *False Claims in Spam*, Apr. 30, 2003, *at* http://www.ftc.gov/reports/spam/030429spamreport.pdf.

[9] *See e.g.*, Anick Jesdanun, *Deleting Spam Costs Billions, Study Finds*, A.P. NEWSWIRES, Feb. 2, 2005 (citing Rockbridge Associates, Inc., *2004 National Technology Readiness Survey Summary Report* (2005), *at* http://www.rhsmith.umd.edu/ntrs/NTRS_2004.pdf).

[10] Nucleus Research, *Research Note D59, Spam: The Silent ROI Killer* (2003), *at* http://www.nucleusresearch.com/research/d59.pdf. *But see* Katie Hafner, *Delete: Bathwater. Undelete: Baby*, N.Y. TIMES, Aug. 5, 2004, at G1 (noting the experience of an author of several Internet books who receives about 900 junk messages a day).

[11] Chris Gaither, *Marketers Hope Antispam Law Restores Industry's Reputation*, BOSTON GLOBE, Dec. 1, 2003, at C1.

[12] Zeller, *Marketers Hope Antispam Law Restores Industry's Reputation*; s*ee also* Postini Resource Center, *Email Stats*, *at* http://www.postini.com/stats/index.php (last visited June 7, 2005) (showing 82.6% of messages processed that day were spam).

open spam messages), private legal steps (such as trespass or breach of contract suits), and public legal reforms (such as laws prohibiting unsolicited commercial electronic mail messages). Thus far, these measures have proven insufficient in stemming the tide of unwanted data.[13]

Why haven't laws prohibiting spam been more effective? A key challenge to legal regulation of spam has been the mobile, commonly cross-border nature of this type of communication.[14] Unlike most problems, spam can easily affect a state's citizens without any physical presence in that jurisdiction: a sender can transmit unwanted messages from outside its borders, with the only contact a stream of bits flowing across the network. A spammer in Boca Raton, Florida in the United States can use a server in China to transmit messages to e-mail users in Malta, Chile, or Estonia. Thus, to enforce a system's legal dictates, spam regulators must work with counterparts in other jurisdictions – an exercise that is complicated not only by differences of language and culture, but particularly by differences in legal process, definitions, and offenses.

One possible approach to this challenge is the harmonization of legal regulation of spam across jurisdictions and borders (to the extent possible). This paper looks at the benefits and difficulties of a "model law" approach to spam, analyzes the key components of spam legislation by highlighting areas of congruence and zones of disagreement, sets forth tentative recommendations for important aspects of any model law, and examines whether such a law would be possible and effective.

D. Evaluating Model Spam Legislation

"Spam" is a contested term; it means different things in different systems. In some legal regimes, there are no express controls on electronic communication; instead, users must depend on related, general-purpose laws, such as those dealing with fraud or consumer protection, or upon non-legal methods, such as filtering. Jurisdictions that legislate controls on spam differ in their definitions of the problem, the locus of control (for example, senders versus advertisers), the actors authorized to enforce these laws, and the penalties that apply to violators. The consequence of this variation is clear: if a spammer in one jurisdiction does not have a physical presence or assets in the jurisdiction where recipients are located, that "target" jurisdiction will have difficulty enforcing its controls on his communications. For example, Malta does not permit senders to transmit unsolicited communications by electronic mail to natural persons without their consent, while the United States permits unsolicited communications until the recipient indicates she no longer wishes to receive them.[15] Thus, the activities of the Boca Raton spammer described above would violate Malta's laws on spam, but not those of the United States. Absent a treaty permitting reciprocal enforcement with the United States, Malta would have difficulty making its prohibition effective with regard to this sender. Coordination of spam legislation can accordingly make

---

[13] *See, e.g.,* Jonathan Krim, *E-Mail Authentication Will Not End Spam, Panelists Say*, WASHINGTON POST, Nov. 11, 2004, at E1; John P. Mello Jr., *CAN-SPAM Compliance Hits New High of 6 Percent*, TECHNEWSWORLD, Dec. 14, 2004, *at* http://www.technewsworld.com/story/news/38945.htm (noting that only 6% of e-mail messages tracked by MX Logic in November 2004 met the requirements of the U.S. spam law); Graeme Wearden, *UK Law Failing to Nail Spammers*, ZDNET UK, Dec. 13, 2004, *at* http://news.zdnet.co.uk/internet/ecommerce/0,39020372,39181034,00.htm (stating that "not a single prosecution has been brought under the Privacy and Electronic Communication regulations and none is imminent" in the U.K.).

[14] *See US Still King of Spam*, AUSTRALIAN IT, Apr. 8, 2005, *at* http://australianit.news.com.au/articles/0,7204,12791070%5E15318%5E%5Enbv%5E15306,00.html (reporting that security company Sophos found 36% of spam between January and March 2005 originated in the U.S., with 25% from South Korea, 10% from China, 3% from France, Spain, and Canada, and 2% from Japan and Brazil).

[15] *Compare* §10(1), *Processing of Personal Data (Electronic Communications Sector) Regulations, 2003* (Malta) (prohibiting use of a publicly available telecommunications service to make an unsolicited communication for the purpose of direct marketing via electronic mail unless the subscriber has given prior express consent in writing), *available at* http://www.dataprotection.gov.mt/filebank/LN16-2003.pdf, *with* 15 U.S.C. § 7704(a)(4) (2004) (United States) (requiring senders to cease sending mail within the scope of a recipient's "opt out" request within ten business days of receiving the request).

such laws more effective by increasing uniformity, decreasing the challenge of complying with inconsistent provisions, and placing senders on notice of permitted and proscribed conduct.

Moreover, this variation in legal controls and the increasing access to information and communication technologies (such as broadband) worldwide encourage spammers to locate their operations in states that have minimal or non-existent penalties for this behavior. This race to the bottom creates at least two problems. First, it helps senders evade legal controls. By operating in an unconstrained fashion, such senders may have a competitive advantage over law-abiding advertisers; if so, this reinforces the incentive to move spam operations offshore. Second, variation can create incentives for countries to adopt weak laws for spam (or not to enact any laws at all), as doing so can mean pecuniary benefits from having domestic "spam hosting" services.

The goal of harmonizing spam legislation in different regimes – for example, through adoption of a "model spam law" – is to simplify and enhance enforcement, and to specify clearly prohibited conduct with the hope of reducing spam's problems. In theory, aligning spam laws across legal systems could have the following benefits:

- **Clear guidelines** – Senders who want to comply with applicable legal requirements could more easily learn what rules apply and could follow them more cheaply, since they would not have to tailor 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 and implementation.
- **Enhanced enforcement** – Regulators could enforce laws more effectively and easily since their systems would share harmonized definitions of offenses, burdens of proof, exceptions, and cooperative arrangements.
- **Stronger norms** – Broad international consensus on the meaning of spam and what constitutes unlawful communication would strengthen norms that deprecate such conduct.
- **Fewer havens for spammers** – As more regimes adopt the model law, spammers would have fewer locations friendly to unlawful activity where they could establish operations, thereby increasing their costs and reducing the financial incentives to engage in this behavior. In addition, harmonized legal provisions will increase pressure on systems to adopt meaningful regulations rather than loose ones that facilitate a domestic spam hosting industry.
- **Increased sharing of best practices** – Since legal systems would share harmonized provisions, regulators and enforcers could more easily collaborate upon, develop, and share best practices for implementing spam laws.

Thus, there are numerous benefits to harmonizing the laws that govern spam in different legal systems. This paper examines aspects of such regulation that seem immediately amenable to such alignment, and also highlights key areas where legal systems differ significantly in order to clarify challenges to harmonization. Finally, the paper looks briefly beyond harmonization to evaluate how effective a harmonized law would likely be, how its efficacy could be maximized, and what other, non-legal modes of regulation should be components of this solution.

II. Key Factors in Regulating Spam Through Legislation

When regulators undertake to control unwanted flows of electronic communication through legislation, they are immediately confronted with several key challenges. How they address these issues and how they frame the problem itself will determine the success of their efforts. The critical issues and decision points are the following:

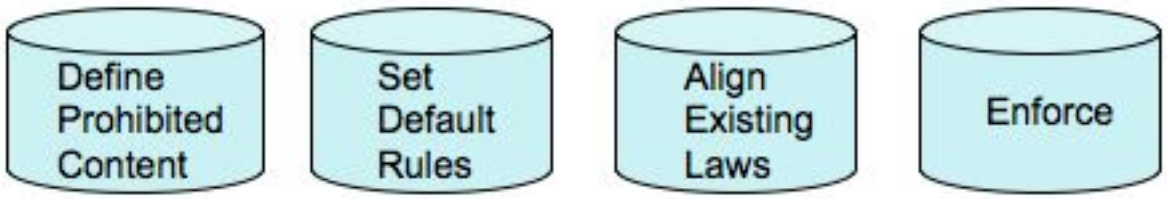

Figure 1 - Key Issues for Spam Legislation

These four categories represent the key decisions regulators must make for legal controls governing spam in any legal regime. Each decision involves a number of important sub-issues; we explore these briefly to acquaint the reader with the considerations involved:

E. Defining Prohibited Content

The first and most important question for regulators is to define the communication they seek to control. What makes an e-mail message, a posting on a Web log ("blog") in a comments field, changes to a Wiki, or an instant message subject to regulation as spam? Typically, rulemakers consider characteristics such as:

- **Bulk transmission** – Is the communication sent only to a small number of recipients (particularly those previously known to the sender) or to a large number of recipients? Does the list of recipients include fictitious or randomly generated addresses?
- **Purpose** – Does the message propose a commercial transaction or otherwise evince a for-profit motive? Is the recipient supposed to take action based on the message?
- **Method** – How is the message transmitted to the recipient (e.g., electronic mail, Simple Message Service (SMS), telephone, etc.)?
- **Truthfulness** – Does the message attempt to mislead or defraud the recipient? Does it conceal the sender's identity or the path that the message took to reach the recipient?

Resolving these questions defines the scope of communication to which the regulations apply. The answers depend in part upon how regulators view the problem (for example, whether the issue is one of

data privacy or one of misuse of electronic mail) and on other laws that bear on these questions (e.g., regulation of unsolicited telephone calls or consumer protection laws).

F. Setting Default Rules for Contacting Recipients

The second question is what rules senders must follow by default in contacting recipients. These include not only abiding by restraints on transmitting prohibited content, but also factors such as:

- **Unsolicited communication** – Can senders contact recipients without advance permission? (The opt-in / opt-out divide between anti-spam systems is perhaps the most fundamental fault line.)
- **Refusing future messages** – Must senders provide a method for, and abide by the decision of, recipients to indicate that they do not wish to receive future messages from this sender or on this topic? Are senders required to delete addresses for recipients who unsubscribe? May senders share such addresses with others?
- **How senders gather recipient data** – Can senders cull recipients' contact information from sources such as Web pages or Internet chat rooms? Can senders construct addresses through random combinations of letters and numbers (similar in effect to using an automatic dialing machine for telephone calls)?
- **Labeling message content** – Must senders indicate a message's contents through methods such as labels or specified subject lines?

G. Harmonizing Existing Laws

Regulation of spam frequently overlaps with existing laws governing aspects of electronic communication or the content often found in spam. Regulators must decide how to align spam regulation with these laws. Relevant questions include:

- **One Law or Many** – Should the legal system adopt legislation specific to spam, or rely on regulation that addresses piecemeal the various aspects of its problems? Or can laws of general applicability, such as those that prohibit various forms of fraud or abuses of consumers, suffice?
- **Rationalizing provisions** – When the issue of spam falls under multiple, potentially conflicting or redundant regulations, how should this conflict be resolved?
- **Reconciling theories** – How can a particular approach to spam controls be aligned with the approaches to issues such as data protection, privacy, consumer protection, computer misuse, and fraud?

H.

Enforcing Rules

Finally, regulators must determine how to effectively enforce their spam controls. Enforcement is the challenge confronting every spam regime.[16] The technical and jurisdictional challenges of Internet-based communication require substantial resources for genuine enforcement and deterrence.[17] Key questions include:

- **Enforcement responsibility** – Who is responsible for enforcing spam laws? How is this responsibility divided vertically (for example, between national and regional authorities) and horizontally (for example, between a data protection agency and police charged with attacking financial crimes)? What roles do private enforcers, such as service providers and end users, play?
- **Coordination** – If more than one enforcer within a given state has jurisdiction over spam offenses, how will these entities coordinate investigations and actions to avoid redundancy and to ensure maximal effectiveness? How will the enforcer(s) coordinate their actions with their counterparts in other jurisdictions, both when the alleged offender is in their jurisdiction and when the alleged victims are there but the sender is abroad?
- **Breadth of liability** – Who is responsible for spam offenses? If there is secondary liability (such as for the entity advertising through the communication or for the creator of software used for the transmission), what standard is required to be liable? What exceptions or defenses exist?
- **Penalties** – What penalties are imposed for violation of spam laws? Who determines and assesses the penalties? What rights of appeal are available? When, if ever, are criminal sanctions employed? How are repeat offenders and multiple violations treated? Are pre-emptive methods, such as injunctions, available, and under what requirements?
- **Jurisdiction** – Under what conditions are the regime's spam laws triggered? Is there extraterritorial application and, if so, when?

Enforcement is the most vital and difficult issue that regulators must address. This is true because spam is amenable to legal regulation at multiple points of control.[18] Responsibility for blocking, avoiding, or otherwise controlling unwanted commercial messages can be placed upon the entity producing the advertised product or service, the message sender, the sender's mail service provider, intermediary Internet service providers (ISPs), the recipient's mail service provider, the recipient, or some combination of these. Moreover, laws may address secondary liability, such as for those who encourage violations of spam laws, produce software that creates and transmits messages, or create tools to compile addresses by searching locations such as Internet news groups or by creating them through combinations of letters and numbers. The challenge for regulators is to determine which set of legal responsibilities produces the greatest effect at the lowest possible cost. Since spam is technologically similar even in different countries, a model law approach can reduce the cost of making these determinations by offering a coherent, pre-drafted legal framework for reducing spam.

[16] See, e.g., Grant Gross, *CAN-SPAM Law Seen as Ineffective*, COMPUTERWORLD, Dec. 27, 2004, *at* http://www.computerworld.com/printthis/2004/0,4814,98559,00.html (noting that the sponsor for the U.S. spam law "has said from Day 1 that enforcement is key for this legislation to be effective").
[17] *See generally* Matthew B. Prince, *Countering Spam: How to Craft an Effective Anti-Spam Law* 6-8, *available at* http://www.itu.int/osg/spu/spam/contributions/Background%20Paper_How%20to%20craft%20and%20effective%20anti-spam%20law.pdf.
[18] *See generally* Jonathan Zittrain, *Internet Points of Control*, 44 B.C. L. REV. 653, 656-59 (2003).

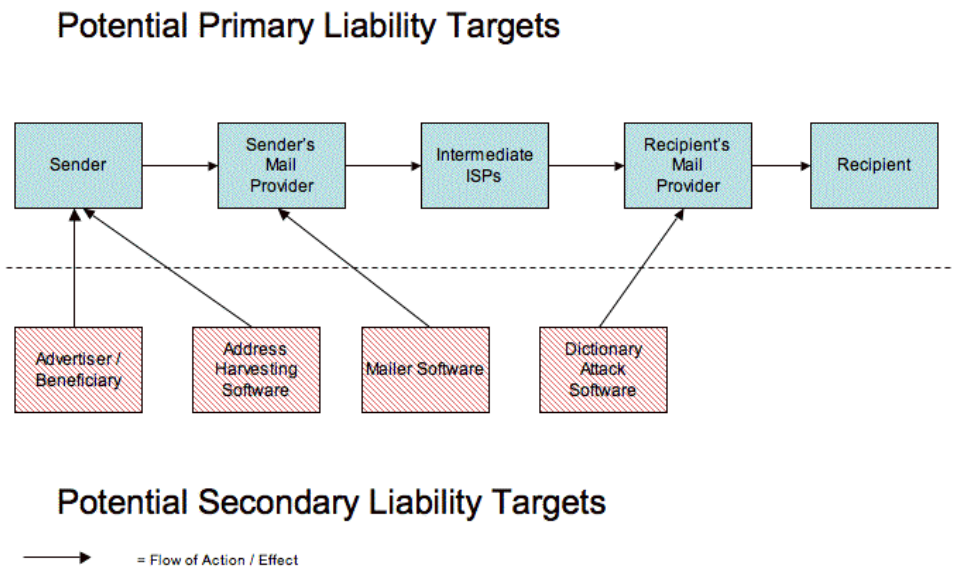

Figure 2 - Potential Points of Control

I. The Limits of Law, and The Need for Other Modes of Regulation

It is a truism in Internet policy that law is only one means of controlling behavior, and rarely the most effective method at that.[19] As the participants in the ITU's Workshop on Spam in July 2004 made plain repeatedly, regulation in the classic legal sense must be seen as only one of the anti-spam tools.[20] Changes in technology, in the markets, and in social norms must also be leveraged if spam is to be controlled. Spam laws, like all legislation, face certain challenges in controlling behavior on-line. Laws ordinarily prompt action after the fact to sanction offenders; thus, once legal penalties are applied, harm has generally already occurred. The effectiveness of legal controls depends on exogenous factors such as enforcement resources, access to proof, defendants' skill and quality of counsel, violators' expectations of being sanctioned, and even luck. In combination, these constraints set an upper bound on how effective laws governing spam can be, even when skillfully crafted and vigilantly enforced.

Regulators must, therefore, be more creative in the online context than they are accustomed to being in ordinary circumstances. Regulators must consider how their traditional laws interact with other modes of governing behavior, including the use of technological restrictions implemented through software code, economic incentives via market mechanisms, and social controls brought to bear through norms.[21] We

[19] *See generally* Lawrence Lessig, *The New Chicago School*, 27 J. LEGAL STUD. 661, 662-66 (1998); Lawrence Lessig, CODE AND OTHER LAWS OF CYBERSPACE (1999).
[20] *See* § 8, *Chairman's Report: ITU WSIS Thematic Meeting on Countering Spam*, July 2004, *at* http://www.itu.int/osg/spu/spam/chairman-report.pdf.
[21] *See, e.g., Spammers Face Big Fines*, NEW ZEALAND HERALD, Feb. 5, 2005, *at* http://www.nzherald.co.nz/index.cfm?c_id=5&ObjectID=10112449 (quoting New Zealand Information Technology Minister David Cunliffe as stating that "No one is pretending legislation is or should be the only part. It has to be a package, there have to be sanctions to back up filters and firewalls").

explore the application of these modalities later in this paper, but mention them here to offer both caution, in considering how effective spam laws can be, and hope, in evaluating supplements to legal regulation.

III. A Typology of Existing Spam Laws

A. Introduction

In considering how to create a model spam law, it is useful to examine existing legislation dealing with spam. The diversity of approaches exhibited by different countries provides a set of building blocks for a model law. In addition, it provides material for analyzing how feasible an effort to harmonize spam laws may be. If different regimes include a core set of elements implemented in similar fashion, alignment becomes easier. Or, if these systems demonstrate widely varying approaches and implementation, harmonization becomes more difficult.

In this section, we distill spam laws into their key component elements, organized under the categories of the four critical decision points outlined above (namely, defining prohibited content, creating default rules, harmonizing existing laws, and enforcing laws). We then evaluate each element on two dimensions; first, we consider how common it is for countries to include that element in their legislation (with a continuum from rare to universal); and second, we analyze how similar the approaches of different countries are with respect to that element (with a range from widely varying to uniform). Thus, this section performs two tasks; first, it describes salient elements from a variety of spam laws passed by individual countries to provide a menu of options for policymakers; and second, it maps these elements based on their commonality and coherence across states to find core features of laws and to highlight areas of agreement and dissonance.

Efforts to create a model spam law or to harmonize existing laws must consider both of these zones. First, elements on which there is general consensus can, and should, be easily included in a model regime or added to systems that do not have them. Second, regulators working to harmonize or to draft model legislation should concentrate their efforts on the thorny issues related to default rules and enforcement. These are not only points on which there are considerable differences between spam regimes, but also ones that must be solved for legislation to be successful.

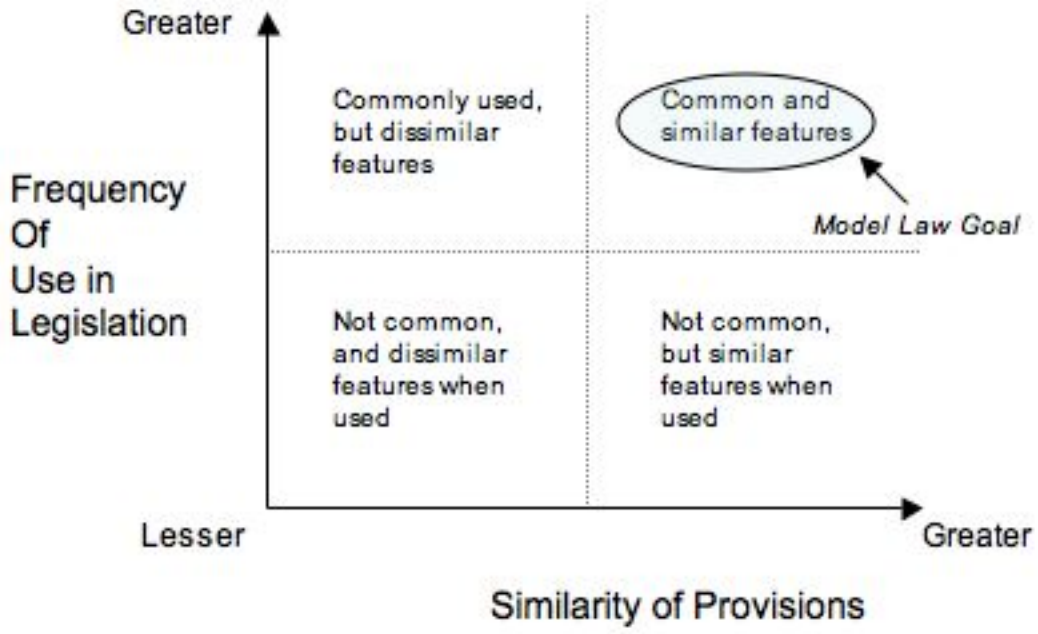

Figure 3 - Typology of Existing Regulation

We now categorize elements of spam laws based on the four key decision points outlined above.

B. Defining Prohibited Content

1) Subject matter: **Common / Uniform**

The initial decision for regulators in assessing spam is whether to differentiate among messages based on their content or purpose. Many spam laws focus on messages that have a commercial purpose; they seek to advertise a product or service to the recipient. For example, Japan's spam laws apply only to for-profit organizations or individuals engaged in a business.[22] This is in contrast to proposals that seek to classify spam as any message transmitted in bulk to recipients who have not requested it.[23]

An important factor in this decision is the larger legal context. For example, the rights afforded to political speech under the United States Constitution limit the ability of U.S. regulators to address unsolicited political messages, while Australian spam laws expressly do not apply if they affect the

[22] *See* Ministry of Internal Affairs and Communications, *MIC announces state of research and development of technology to help prevent trouble from the transmission or reception of spam and the introduction of these by telecommunications carriers providing services related to email*, Dec. 27, 2004, *at* http://www.soumu.go.jp/joho_tsusin/eng/Releases/Telecommunications/news041227_8.html.
[23] *See, e.g.,* Coalition Against Unsolicited Bulk Email, Australia, *Definitions of Words We Use*, *at* http://www.caube.org.au/whatis.htm (last visited June 7, 2005) (defining spam as unsolicited bulk e-mail regardless of its content).

constitutional right of political communication.[24] In addition, the profit motivation for unsolicited commercial messages is often cited as a rationale for focusing on this type of content.

Some regimes make a distinction among commercial messages based on the relationship between recipient and sender. For example, a system might permit a merchant who has previously sold goods to a consumer to contact that consumer by e-mail to advertise a new version of those goods. We discuss this "soft opt-in" approach under Section C below.

2) Applications Covered: **Common / Varying**

Spam messages are a challenge in many communications media, from postal mail to voice telephone calls to electronic mail. Regulators must decide whether to deal with spam only in the context of e-mail, or whether to specify that laws cover other applications, such as Short Messaging Service (SMS) text messages on cellular phones, instant messaging (known as "spim")[25], blogs, and RSS. Some spam laws, such as the European Commission's Directive 2002/58/EC, are application-agnostic and cover all methods of electronic communications.[26] Other laws, such as those of the United States, apply only to electronic mail and, for example, communications by SMS are governed by separate regulations.[27] Indeed, the advent and growing popularity of Voice over Internet Protocol (VoIP) for telephony will likely confront regulators dealing with unsolicited communications with the convergence of IP-based systems, such as the Internet and circuit-routed systems (e.g. standard telephone service). Thus, specifying the media to which a regulation applies is common, but the choice of media to cover varies from system to system.

[24] *See* Art. I, U.S. Constitution; § 44, *Spam Act 2003* (Australia).
[25] *See* Joseph Menn, *N.Y. Man Arrested Over Instant-Message Spam*, LOS ANGELES TIMES, Feb. 19, 2005, at A1 (noting that spim constitutes 1% of traffic on AOL Instant Messenger and that this number is expected to increase); Robert MacMillan, *Spammers Seeking Out Instant Messengers, Survey Shows*, WASHINGTONPOST.COM, Feb. 22, 2005, *at* http://www.washingtonpost.com/wp-dyn/articles/A45011-2005Feb22.html (noting that one-third of Americans who use instant messaging software have received spim at least once and that instant messaging software development firm IMLogic found that 5% of instant messages in 2004 were SPIM). A recent study by the University of St. Gallen in Switzerland found that 80% of mobile users had received spam. *See* Institute for Media and Communications Management, *First Empirical Global Spam Study Indicates More Than 80 Percent of Mobile Phone Users Receive Spam*, Feb. 9, 2005, *available at* http://www.ntu.edu.sg/sci/sirc/download/PR%20Mobile%20Spam%20Study.pdf.
[26] *See* Art. 2(h), Council Directive 2002/58/EC, 2002 O.J. (L 201) 37, 43 (European Union).
[27] *See Rules and Regulations Implementing the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003; Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991*, § A of "Discussion," 69 Fed. Reg. 55,765 (Sept. 16, 2004) (to be codified at 47 C.F.R. pt. 64) (United States) (stating that "phone-to-phone SMS is not captured by section 14 of the CAN SPAM Act because such messages do not have references to Internet domains" and that that the Telephone Consumer Protection Act's "prohibition on using automatic telephone dialing systems to make calls to wireless phone numbers applies to text messages.").

3) Fraudulent / Misleading Information: **Common / Uniform**

Most legal regimes, regardless of how they configure spam laws, prohibit messages that contain fraudulent, deceptive, or misleading information. Such bans typically target one or more of:

- the sender's identity, e-mail address, or affiliation
- the opt-out address used to refuse further communications
- the material advertising or offering goods or services
- the purpose of the message
- the routing path of the message (including message headers)
- the message subject line

These prohibitions are important to the functioning and purpose of spam legislation. If senders are permitted to defraud recipients, consumers will become less willing to engage in electronic commerce. If opt-out addresses are not functional, recipients cannot choose what advertising they receive and what they reject. If the advertiser's identity is concealed, reputational penalties for behavior are reduced. Fraudulent messages comprise an increasing problem even within spam, as the wave of "phishing" attacks proves.[28] Messages using fraudulent sender addresses harm innocent third parties who may suffer significant reputation harm. When consumer complaints are erroneously sent to a third party victim, significant cost is also created.

Prohibitions on fraudulent information in spam-specific legislation often overlap with laws that ban fraudulent or deceptive practices. For example, the European Union addresses fraudulent or deceptive advertising under Directive 84/450/EEC.[29] Peru prohibits the use of a false identity in e-mail messages and the falsification of data under its criminal laws.[30] The value of additional provisions targeted at spam is that some portions of spam – such as the return address or routing path – may not be covered by existing laws governing fraud or misleading advertising. These items, though, are vital to tracing spam and to identifying its senders; thus, prohibiting falsification is important.

C. Setting Default Rules for Contacting Recipients

1) Opt-In versus Opt-Out: **Common / Varying**

As an initial matter, regulators must determine whether unsolicited messages are permitted or forbidden. If they are permitted, the system is an opt-out one; if prohibited, the system is opt-in (This paper assumes that regulators addressing spam would, in a system where unsolicited messages are permitted, actively seek to reinforce legally recipients' decisions to opt out of receiving messages from particular senders or on particular topics from a sender and, in a system where unsolicited messages are forbidden, seek to enable recipients to receive messages to which they have specifically consented.) Further, regulation depends greatly upon this choice, as opt-in regimes will focus on the means of obtaining, recording, and revoking consent, while opt-out regimes will concentrate upon methods for indicating that one does not wish to receive messages, requirements for storing such preferences, and methods of enforcing this choice. This initial choice defines what a legal regime considers "spam": is it unsolicited messages, or only unsolicited messages that meet (or contravene) further provisions?

[28] *See, e.g.,* Anti-Phishing Working Group, *at* http://www.antiphishing.org/; Brian Krebs, *Despite Efforts to Contain Them, "Phishing" Scams Spread*, Washington Post, Jan. 19, 2005, at E5.
[29] Council Directive 84/450/EEC, 1984 O.J. (L 250) 17.
[30] Arts. 161, 427, Criminal Code (Peru).

This decision is a key fault line in existing spam regulation. The United States, South Korea, and Colombia employ the opt-out system. This sets a default position that permits senders to contact recipients who have not granted prior permission. In contrast, Australia and the European Union use the opt-in system. This default rule forbids senders from contacting recipients unless the recipient has indicated prior consent. Thus, there are serious, sustained efforts to treat the spam problem under both potential default rules. The challenge to harmonization is that this element is almost always a key part of the definition of spam: either senders must obtain recipients' permission or not. While a model law could allow adopting states to make their own decision on this element, doing so would weaken consistency and enforcement since messages sent from an opt-out regime would not (absent a reciprocal enforcement agreement) constitute an offense, even if sent to a recipient in an opt-in jurisdiction.[31] Any anti-spam regime with an opt-in system at its core is almost certain to be a more aggressive anti-spam regime than an opt-out system. This divide in existing provisions will constitute a major issue with which harmonization must contend.

2) Opt-In Exception - Existing Relationship: **Common / Uniform**

Even in legal regimes that ban unsolicited messages, it is common to create an exemption for a business entity with which the recipient has previous or on-going dealings. This provision is often referred to as a "soft opt-in." It is often coupled with two requirements: that the business allow the recipient to opt out of receiving such messages when her personal data is collected during the initial contact or transaction, and that subsequent messages include a way to opt out of future communication. For example, the United Kingdom permits unsolicited direct marketing by e-mail when the recipient's contact data was collected during the sale or negotiations for goods or services, provided that the marketing is for similar goods or services and that the recipient was allowed to refuse (at no charge) such marketing at the time of collection and that she does not withdraw permission for such communication when messages are sent.[32] Malta has similar provisions.[33] The "soft opt-in" is required of European Union member states under Directive 2002/58/EC.[34] The rationale for such an exception is that the consumer has already indicated interest both in this type of transaction and in this sender; thus, consent to receive additional and similar communications is implied.

3) Mandatory Disclosure: **Common / Uniform**

Spam regulations frequently mandate that the message's sender disclose certain identifying information to the recipient. For example, South Korea requires that the sender include the message's objective and major contents, her name and either address or telephone number, the source from which the recipient's e-mail address was obtained, and instructions on how to opt out of future advertising messages.[35] Mexico instructs senders to include their name, address, and telephone number, along with those of the business on behalf of which the message is sent and also the information on the Office of the Federal Attorney for

[31] We note that states could, in theory, provide that under an opt-out system, messages sent to recipients in locations governed by opt-in regulations would be unlawful. However, this would provide different (and arguably stricter) protection for non-citizens than for citizens, which would seem unlikely in practice.
[32] *See* § 22, *The Privacy and Electronic Communications (EC Directive) Regulations 2003* (2003), SI 2003/2426, *available at* http://www.opsi.gov.uk/si/si2003/20032426.htm (United Kingdom).
[33] *See* Art. 10(2), *Processing of Personal Data (Electronic Communications Sector) Regulations, 2003* (under the Data Protection Act (CAP. 440), L.N. 16 of 2003) (Malta), *available at* http://www.dataprotection.gov.mt/filebank/LN16-2003.pdf.
[34] *See* Arts. 13(2), 17, Directive 2002/58/EC, 2002 O.J. (L 201) 37, 45-47; *see also* § 2.1, Commission of the European Communities, *Communication on Unsolicited Commercial Communications or "Spam,"* COM(2004)28 final at 9-10 (Jan. 22, 2004).
[35] *See* Art. 50(2), *Act on Promotion of Information and Communication and Communications Network Utilization and Information Protection of 2001* (as amended by Act No. 6797, Dec. 18, 2002) (South Korea), *available at* http://www.mic.go.kr/eng/res/index.jsp.

Consumer Protection.[36] These mandatory disclosure elements serve several purposes. First, they allow recipients to learn easily who is responsible for sending them a message. Second, by tying a business or individual's identity, and therefore reputation, to a message, the requirements encourage senders to behave responsibly. Third, the information aids enforcement actions by recipients or regulators. Finally, disclosures may enable more effective filtering of spam messages by allowing recipients to block messages containing a given sender's name, phone number, or other identifying information. The effectiveness of disclosure provisions depends on the existence and enforcement of prohibitions upon falsifying or omitting this information.

4) Means of Acquiring or Producing Recipient Addresses

Spam laws often regulate how senders and the entities on behalf of whom they advertise may acquire, produce, and use e-mail addresses. There are two primary concerns in this area.

a) Address harvesting: **Common / Uniform**

First, senders may search the Internet – including Web sites, blogs, chat rooms, and Usenet news groups – to locate and compile e-mail addresses. Thus, by listing one's e-mail address as a contact method on a Web site or by participating in an on-line discussion forum, a user may increase her likelihood of receiving spam. The concern for this "address harvesting" is that it inhibits the use of e-mail addresses on the Internet as a contact method and subjects users who employ their address in an unrelated context to a barrage of spam. The use of address harvesting tools is often forbidden. The United States, for example, prohibits sending commercial e-mail to recipients whose addresses were obtained through automated means from a Web site that states it does not make e-mail addresses available for the purpose of sending mail.[37] Gathering addresses in this fashion – whether manually or via software tools – is generally unlawful under the European Union's Data Protection Directive (Directive 95/46/EC). Many other countries have similar data protection or data privacy legislation that forbids such address acquisition and aggregation.

b) Dictionary attacks: **Uncommon / Uniform**

Second, spammers often generate target e-mail addresses by combining letters and numbers to form likely addresses; for example, a sender might build an address list by iterating "johndoe1@yahoo.com", "johndoe2@yahoo.com", and so forth. Software programs can automate this process and employ algorithms to create more realistic addresses than random generation would produce. Spammers then attempt to transmit messages to each of these addresses, even though many if not most do not correspond to actual users. This produces two detrimental effects. The large number of inaccurate addresses places a considerable load on the servers of mail service providers with no corresponding benefit: it is equivalent to receiving a massive volume of "wrong number" calls on one's telephone. In addition, it causes messages that are successfully transmitted to be poorly targeted, since the recipient is randomly selected. Transmitting messages to addresses created in this manner is often banned. South Korea, for example, prohibits using any program that creates recipient contact information, such as e-mail addresses or telephone numbers, by combining letters, marks, and numbers.[38]

c) Software tools for address harvesting / dictionary attacks: **Common / Uniform**

[36] *See* Art. 17, *Federal Law for Consumer Protection*, *available at* http://www.profeco.gob.mx/html/ecomercio/ecomercio_lfpc.htm (Mexico).
[37] 15 U.S.C. § 7704(b)(1) (2004).
[38] Art. 50(6), *Act on Promotion of Information and Communication and Communications Network Utilization and Information Protection of 2001.*

Spam laws that prohibit address harvesting and dictionary attacks often ban the creation and use of software that performs these functions as well. Japan prohibits programs that generate random, fictitious addresses.[39] Moreover, the use of or transactions in lists compiled using such software are often banned. South Korea bans using, distributing, or selling addresses gathered using such software tools if the user knows that the collection of the addresses violated the prohibition on aggregating them from Web pages against the terms of service on those pages.[40] The goal of these bans is to make sending spam more difficult by reducing the number of automated tools that produce addresses. Secondary liability is important because it is faster and easier for a spammer to purchase lists of e-mail addresses than to collect them (either manually or using software tools). Thus, banning the use and sale of lists gathered with such tools helps prevent spammers from dodging liability.

d) Publicly disclosed addresses: **Uncommon / Varying**

Some e-mail addresses are made publicly available because the recipient seeks communication from the general public (such as a political candidate posting an address on her campaign Web site, or the ombudsman for a newspaper posting her address on the newspaper's site). Spam laws treat these addresses differently. South Korea prohibits gathering and using e-mail addresses posted on Web sites only if the sites post terms prohibiting such collection and use.[41] Argentina's Personal Data Protection Act would seem to permit collection of e-mail addresses (which qualify as personal data under the Act) if the addresses are posted on publicly-available Web sites.[42] The assumption of these provisions is that recipients have implicitly consented to receive unsolicited messages. Thus, existing regimes treat publicly disclosed addresses differently in terms of whether their collection and use is prohibited.

e) Requirements to destroy / remove addresses: **Uncommon / Uniform**

Once a recipient has indicated that she no longer wishes to receive communications from a particular sender, the sender may be legally obligated to expunge information (such as her e-mail address) from its records. Argentina permits recipients to demand that a sender remove their addresses from the sender's database.[43] Removal requirements often comport with a legal system's data protection laws. Such a mandate may be more applicable to an opt-in regime, where only recipients who have consented may be lawfully contacted, than an opt-out regime, where senders might need to retain e-mail addresses for users who unsubscribe in order to track to whom messages should not be sent.

5) Unsubscribe Requirement: **Common / Similar**

a) Inclusion

Spam legislation often contains a requirement that the message sender include a means by which the recipient can indicate that she no longer wishes to receive messages from that sender or on that topic, along with a mandate that the sender adhere to the recipient's wishes. For example, Argentina compels senders to honor unsubscribe requests by recipients.[44] This feature often comports with a state's approach to data protection and privacy generally by giving the recipient control over the retention and use of her e-

[39] *See* Ministry of Internal Affairs and Communications, *"Study Group on Countermeasures against SPAM" Held*, Nov. 2, 2004, *at* http://www.soumu.go.jp/joho_tsusin/eng/Releases/NewsLetter/Vol15/Vol15_15/#3 (Japan).
[40] *See* Arts. 50-2(1), 50-2(2), *Act on Promotion of Information and Communication and Communications Network Utilization and Information Protection of 2001.*
[41] Arts. 50-2(1), 50-2(2), *Act on Promotion of Information and Communication and Communications Network Utilization and Information Protection of 2001.*
[42] See § 5(2)(a), Law No. 25326, Oct. 4, 2000, *available at* http://www2.jus.gov.ar/dnpdp/ley.html (Spanish).
[43] § 27(3), Law No. 25326.
[44] § 27(3), Law No. 25326.

mail address. Unsubscribe requirements are particularly important for opt-out regimes since they provide the means by which recipients control whether they receive commercial messages. This method, though, is also useful for opt-in systems since it allows a recipient to change her mind by revoking permission to communicate with her in this fashion.

b) Method

Legislation may be neutral in the method that an unsubscribe function may take or it may prescribe one or more ways in which recipients must be able to communicate with the sender for this purpose, such as through a working e-mail address, a phone number, or a URL leading to a form for such requests. Australia requires that senders provide opt-out functionality using the same technology with which the message was sent – for example, an advertising message transmitted by e-mail must allow the recipient to unsubscribe by e-mail.[45]

c) Characteristics

Laws may also dictate characteristics of the unsubscribe method. The United States requires that a sender's unsubscribe mechanism function for at least thirty days after the message was sent.[46] Provisions preventing senders from imposing costs on recipients who opt out are common. South Korea requires senders to take measures to avoid creating such expenses and to reimburse recipients who incur them and Australia prohibits unsubscribe mechanisms that use a premium service.[47] Laws may specify which languages the unsubscribe mechanism must employ, such as requiring that the method use the country's official language(s), English, or both.

d) Effects

Unsubscribe requirements require two things to be effective. First, senders must honor the request. Some senders may ignore such responses from recipients or may seek to evade them – for example, by closing the e-mail address used to gather such requests rapidly and shifting to a new one. Second, recipients must have sufficient confidence in the efficacy of unsubscribe methods to use them. Currently, most advice on spam cautions users against employing unsubscribe functions due to fears that senders will not comply with these requests and that attempting to unsubscribe will confirm that the recipient has received (and read) the message.[48] Indeed, there is a thriving market for e-mail addresses of recipients who actually open (and respond to) spam messages.[49] This may make unsubscribe requirements more effective in opt-in schemes than in opt-out schemes; users are more likely to remember which senders they permit to transmit messages to them and thus can employ unsubscribe features for these senders while ignoring opt-out options from non-compliant senders. In addition, it is important to prevent senders from transferring or sharing this recipient's address; otherwise, senders can lawfully compile and sell lists of recipients

[45] §§ 3.1-3.3, *Spam Regulations 2004*, Statutory Rules 2004 No. 56, *available at* http://scaleplus.law.gov.au/html/numrul/20/10084/top.htm.
[46] 15 U.S.C. § 7704(a)(3) (2004).
[47] *See* Art. 50(5), *Act on Promotion of Information and Communication and Communications Network Utilization and Information Protection of 2001* (as amended by Act No. 6797, Dec. 18, 2002) (South Korea), *available at* http://www.mic.go.kr/eng/res/index.jsp; § 3.2, *Spam Regulations 2004*, Statutory Rules 2004 No. 56 (Australia).
[48] *See, e.g.,* Bob Sullivan, *New Reason to Avoid "Unsubscribe" Links*, MSNBC, Oct. 8, 2004, *at* http://msnbc.msn.com/id/6208701/ (describing the arguments against using unsubscribe functions, including the risk that URLs used for this purpose may contain code that compromises a user's computer).
[49] The value of a known valid e-mail address has been estimated to be worth as much as $0.50 US each. Federal Trade Commission, *National Do Not Email Registry: A Report to Congress* 18 n.90 (2004), *at* http://www.ftc.gov/reports/dneregistry/report.pdf.

who, in unsubscribing, have proved they open and respond to spam messages.[50] If regulators adopt an unsubscribe provision, they must consider the effects of user attitudes and norms towards this feature, as well as the importance of minimizing the illicit use of unsubscribe functionality by spammers to detect and target active e-mail accounts.

6) Subject Line Requirement

The subject line of an e-mail message typically describes the message's content or context. The subject line is part of the message's body and is generally displayed by a user's e-mail client software along with the sender's name, the sender's address, and the time of receipt in the Inbox view of the user's mail store. Spam messages often contain enticing but false subject lines designed to cause users to open and view the messages. This benefits the spammer in two ways: first, opening the message can reveal that the user's address is active through techniques such as Web bugs[51]; and second, the likelihood that the user will take action based on the message content (for example, by visiting a URL listed in the message) increases if the user actually views the message body.

Accordingly, spam laws often regulate the text of the subject line. These requirements typically contain one or both of two approaches: prescribing that a label is included in the subject line of messages and proscribing subject lines that are false or that are likely to mislead the recipient.

e) Requiring Labels: **Common / Varying**

The first approach seeks to enable users to identify (and filter) spam messages easily by requiring that the subject line contain a distinctive identifier, such as a series of characters. South Korea mandates that advertising messages contain the character "@" in the subject line and that messages with adult content (such as pornography) contain the characters "ADLT". Users who see these characters can immediately identify the messages as advertising or porn. In addition, most software programs that filter e-mail messages to block spam can be set to identify and delete messages with specific characteristics, such as the presence of certain characters in the subject line. Thus, requiring that all spam messages have subject lines containing the characters "ADV" enables users to set their spam filters to delete or quarantine all messages with "ADV" in the subject.

Labeling requirements can benefit significantly from harmonization. Currently, different regimes prescribe different labels – South Korea uses "@", the United States and Singapore have proposed "ADV", and Spain requires labeling messages with "Advertising."[52]

f) Banning Fraudulent or Misleading Subjects: **Common / Similar**

The second approach seeks to prevent users from being misled about the nature, context, or content of a message. This is typically specified as a prohibition against false or misleading subject lines. For

[50] *See, e.g.,* 15 U.S.C. § 7704(a)(4) (2004) (United States) (prohibiting a sender from transferring or sharing the e-mail address of a recipient who "opts out" of receiving messages, except to comply with legal requirements).
[51] *See* Richard M. Smith, *The Web Bug FAQ*, *at* http://www.eff.org/Privacy/Marketing/web_bug.html (Nov. 11, 1999) (describing how Web bugs work and their use in spam messages).
[52] *See* Korean Spam Response Center, Filtering, at http://www.spamcop.or.kr/eng/m_3.html (Korea); 15 U.S.C. § 7710(2) (2004) (requiring the report within 18 months of the Act's enactment and allowing the FTC to recommend compliance with IETF standards, use of "ADV," or no plan at all) (United States); § 5.28(b), InfoComm Development Authority of Singapore – Attorney General's Chambers of Singapore, *Proposed Legislative Framework for the Control of E-mail Spam*, May 25, 2004, *at* http://www.ida.gov.sg/idaweb/doc/download/I2883/Proposed_Legislative_Framework_for_the_Control_of_E-mail_Spam.pdf (Singapore); Art. 20, Law 34/2002, July 11, 2002 (as modified by Law 32/2003), *available at* http://www.setsi.mcyt.es/legisla/internet/ley34_02/sumario.htm (Spain).

example, the United States prohibits using a subject line the sender knows is likely to mislead the recipient. Thus, an unsolicited message advertising software with the subject line "RE: Your request for information" would violate this prohibition. This proscriptive measure attempts to ensure that users can evaluate a message's content before choosing to view it.

g) Effects

One common concern about subject line requirements is that their burden falls primarily on legitimate advertisers who comply with the law while failing to affect non-compliant senders. For example, senders who comply with a labeling requirement risk having their messages filtered by users' mail clients or anti-spam software while advertisers who flout the requirement have an increased likelihood of having their messages received and read. Labeling requirements may increase the volume of non-compliant messages as marginal senders choose to flout the law rather than increase the likelihood that their messages will be deleted by filters. The merits of such requirements depend on an empirical assessment of how frequently users filter messages based on subject lines, how often they respond to messages with misleading subjects, and what level of blocking of compliant messages is acceptable to obtain a given reduction of non-compliant messages. We believe additional, quantitative research would be useful in this area.

D. Harmonizing Existing Laws

Legal systems must align existing regulations with spam laws. These efforts fall into two primary zones. First, regulators must decide whether to use rules specific to spam or whether to rely on broader, more general-purpose laws – in essence, to choose whether to use one law or many to control spam. Second, systems need to reconcile provisions of spam laws with similar or applicable elements of other laws.

1) One Law or Many

There is a clear trend among legal systems to move towards regulations specific to spam. A number of states do not have rules focused solely on spam, relying instead on approaches such as data protection (e.g., Colombia), common law suits (e.g., Russia), consumer protection statutes (e.g., Mexico), and self-regulation by service providers (e.g., China). However, each of these states has introduced or is considering legislation specific to spam. Creating regulations targeting spam in particular can help focus enforcement efforts, strengthen norms against this behavior, and close loopholes or uncertainties in existing laws that also apply to spam.

2) Rationalizing Provisions: **Common / Varying**

Spam holds the potential to fall under a number of different rubrics in terms of legal control, from computer misuse to false advertising to data protection to criminal fraud. Legal systems that implement spam legislation must consider, and hopefully specify, how these different elements will interact. Will penalties under a spam law be exclusive, or is there the possibility for additive civil or criminal liability? The United States has a particularly complicated task in this regard given that it must rationalize both horizontally (across subject areas of enforcement, such as consumer protection) and vertically (between state-level and federal-level legislation). The American CAN SPAM Act permits states to impose liability for criminal violations such as fraud, computer crimes, or civil infractions (e.g. torts or breaches of contract), in addition to penalties that are allowed under the spam law itself.[53] State laws regulating commercial e-mail, however, are not allowed (except to the extent that they prohibit fraud).[54] Similarly,

[53] 15 U.S.C. § 7707(b)(2) (2004).
[54] 15 U.S.C. § 7707(b)(1) (2004).

CAN SPAM aligns its provisions with federal laws, such as those governing computer misuse; these offenses are additive, and a previous violation of the computer misuse law can result in increased penalties for a spam law violation.[55] While a model spam law could not provide for the specifics of rationalizing its provisions with each implementing system's existing legislation, it could contain provisions that require an adopting regime to undertake an effort to analyze and align the new spam regulations with extant ones.

E. Enforcing Rules

Enforcement is one of the most critical components of any framework designed to control spam. States drafting spam legislation must commit to devoting substantial, meaningful state resources to identify, pursue, prosecute, and penalize those who flout these laws if there is any hope that these laws will have any impact. Enforcement is vital to establishing an effective deterrent to unlawful behavior and to raising the practical costs of operating a spamming business. This need for careful investigation and vigorous prosecution applies regardless of the legislative configuration adopted. The challenges to enforcement – including the cross-jurisdictional nature of many spam operations, the technical difficulties of tracking messages, and the risk that spammers may have limited assets to satisfy judgments or fines – are common to opt-in and opt-out regimes. Establishing spam legislation but neglecting enforcement may be worse than doing nothing, as it can provide the appearance of addressing the problem without creating real limits on advertising through electronic communications.[56]

1) Pre-emption: **Common / Varying**

Many regimes will confront the possibility of multiple entities that are potentially competent for or charged with regulating spam. These entities may exist in a vertical relationship (for example, the relationship between territories and a central government in a federal system such as that of Australia or the United States, or between a coordinating body and individual states such as that of the European Union), in a horizontal relationship (for example, between different regulatory agencies, such as the Commission Nationale de l'Informatique et des Libertés (CNIL) and the Générale de la Concurrence, de la Consummation et de la Répression des Fraudes (DGCCRF)), or a mixture of both. Thus, spam regulation must address the relative authority and scope of these entities. Vertically, spam laws can designate the relative roles of central and regional governments. Australia permits states and territories to regulate spam as long as their laws do not contradict those of the Commonwealth.[57] In contrast, the CAN SPAM Act of the United States expressly pre-empts or prevents regulation of commercial e-mail by individual states, with the exception of laws that prohibit falsity or deception in messages or that are not specific to electronic mail (such as civil contract or criminal laws).[58] Thus, regulators must decide how to divide responsibility for the creation and enforcement of spam legislation vertically (where relevant) and horizontally. In both cases, coordination and information-sharing among regulatory entities is vital to the success of such laws.

2) Jurisdiction: **Common / Varying**

---

[55] *See* 18 U.S.C. § 1030 (prohibiting fraud and related activities with computers); 18 U.S.C. § 1037 (prohibiting violations of the CAN SPAM Act); 18 U.S.C. § 1037(b)(1) (imposing a greater sentence for violations when the defendant has a previous conviction for a violation of 18 U.S.C. § 1030 (the Computer Fraud and Abuse Act)).

[56] 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, on the effectiveness of which Prof. Lessig has "bet [his] job." *See* http://www.lessig.org/blog/archives/000787.shtml. *See infra* note 72.

[57] *See* § 43, *Spam Act 2003*.

[58] *See* 15 U.S.C. § 7707(b)(1) (2004).

Jurisdictional elements in spam legislation define the conditions under which the law applies to an electronic message. The packet-based routing of electronic messages over Internet Protocol (IP) means that the bits comprising a message from a sender in Portugal to a recipient in Japan may transit a multitude of other countries on the path between the communicants. Thus, defining which legal regimes may (and want to) regulate that message is vital. The possible jurisdictional "hooks" derive from the diagram on possible points of control in Section II. At minimum, the states where the sender and the recipient are located would likely assert a jurisdictional interest in the message. Additional jurisdictions might be implicated based on the location of

- the messaging service providers and Internet service providers involved
- the computer used to transmit or to access the message
- the entities responsible for or deriving benefit from the message's contents
- the organizations supervising or employing sender or recipient
- the developers of the software used to effect the communication

Existing spam laws display a range of jurisdictional requirements. Ireland's jurisdictional element is narrowly defined, as the message must be sent from within the Republic for a violation to occur.[59] In contrast, Australia's jurisdiction over spam is expansive, affecting any message with an "Australian link."[60] This link occurs when any of the following occurs:

- the message originates there
- the individual who sent or authorized the message is there when the message is sent, or the organization that sent or authorized the message has central management and control in Australia when sent
- the computer used to access the message is in Australia
- the account holder is an individual, or an organization having business or activity in Australia when the message is accessed, or
- if the message could not be delivered because the recipient address did not exist, it is reasonably likely that it would have been accessed from a computer or device in Australia[61]

Of course, jurisdictional elements in spam legislation must comport with relevant external limits – for example, due process requirements of various states' constitutions, or the "mere conduit" exemption from liability for intermediaries established by the European Commission's Directive on Electronic Commerce.[62]

3) Extraterritorial Application: **Uncommon / Varying**

Spam laws may also apply to conduct or entities located beyond the legal borders of the relevant regulating entity. Thus, spam legislation might cover the actions of a state's citizen while she was outside its borders. Australia, for example, specifies that its law "extends to acts, omissions, matters and things outside" the country.[63] Spain claims jurisdiction over entities outside the European Union if their actions threaten public order, and asserts that entities within the EU are subject to the state's spam laws if they direct their services into Spain.[64] Extraterritorial application of spam laws may be helpful in mitigating the ease with which this problem crosses legal boundaries, but it also raises questions of choice and conflict of laws, as well as the effects of such application on cooperative arrangements between different regulating entities or states.

4) Memoranda of Understanding / Cooperative Agreements: **Uncommon / Uniform**

Since spam crosses legal borders efficiently, efforts to control it must do so as well. It is common for spam authorities to enter into cooperation agreements, often instantiated as memoranda of understanding, with their counterparts in other jurisdictions.[65] Harmonized spam legislation or a model law could formalize the basis for such agreements and could commit the implementing legal system to pursue them. Australia specifically authorizes its enforcement body to liaise with foreign regulators to deal with unsolicited commercial e-mail and with address harvesting.[66] The European Union has proposed

[59] *See* Data Protection Commissioner, *Guidance on Unsolicited Electronic Communication*, *at* http://www.dataprivacy.ie/documents/rights/spamGuide.pdf (Ireland).
[60] *See* § 7, *Spam Act 2003*, *at* http://scaleplus.law.gov.au/html/pasteact/3/3628/0/PA000110.htm (Australia).
[61] § 7, *Spam Act 2003*.
[62] *See* Art. 12, Council Directive 2000/31/EC, 2000 O.J. (L 178) 1, 12-13 (defining the "mere conduit" exemption).
[63] § 14, *Spam Act 2003*.
[64] Arts. 4, 8, Law 34/2002, July 11, 2002 (as modified by Law 32/2003).
[65] *See, e.g., Anti-Spam Assault Spans Asia-Pacific*, ZDNET AUSTRALIA, Apr. 28, 2005, *at* http://www.zdnet.com.au/news/security/0,2000061744,39189877,00.htm (describing the signature of the Seoul-Melbourne Anti-Spam Agreement by twelve communications and Internet agencies and the role of the memorandum in sharing information).
[66] § 42, *Spam Act of 2003*.

regulations for enforcing consumer protection provisions across borders, which would enhance enforcement of provisions prohibiting spam that is fraudulent or misleading.[67] Including provisions for cooperative action – for example, by authorizing and directing government enforcement entities to enter into memoranda of understanding – can bolster cross-border enforcement of spam laws.

5) Liability: **Common / Varying**

A critical feature of spam laws is the entity or actor that is liable for violations. Holding the sender of a spam message responsible for breaches of applicable regulations is obvious. However, additional liability provisions can be valuable as well.

For example, a number of existing laws provide for liability not only for the sender, but for the entity advertising products or services through spam. A key element in spam is the financial structure that makes the practice rewarding. The costs of transmitting messages are typically extremely low, especially for e-mail, where the sender can transmit a single message that is eventually delivered to many recipients. These low costs are what make spam remunerative even with response rates as low as one one-hundredth of one percent.[68] Most proposals for mitigating spam seek to increase these costs. In addition, it is helpful to target the revenue earned by spam. This can be done effectively by creating secondary liability for entities that benefit from spam advertising, even if these entities do not themselves transmit the messages. Some spam laws already implement secondary liability. Australia prohibits sending most commercial electronic messages without the recipient's consent and imposes liability on anyone who aids, induces, conspires in, or is directly or indirectly a party to such violations.[69] Similarly, Singapore's proposed legislation would hold "that the merchant or business commissioning or procuring spam should also be liable."[70] Imposing liability on the advertiser should induce businesses to exercise control over their marketing communications. A regime of strict liability may be helpful in this area since businesses can create contractual provisions for indemnification for violations with firms or individuals who transmit their advertising (If there is concern that spammers might send messages without permission purporting to be from legitimate sources, the burden of proof could require that the prosecutor or plaintiff demonstrate a business relationship between the sender and the advertiser through formal agreements or shared revenues.) Conversely, exempting advertisers from liability would encourage businesses to outsource transmission of their marketing messages to avoid incurring penalties; this would encourage the growth of senders who operate beyond effective control by minimizing their assets at risk (such as through shell corporations).

As noted in the discussion of address harvesting and dictionary attacks, many regimes also place secondary liability on entities that create, sell, or employ tools to automate this behavior. As with imposing liability on advertisers, these provisions can increase the costs for and decrease the efficiency of spammers.

Another liability factor is to exempt entities, particularly Internet Service Providers, from liability for their efforts to block spam. South Korea authorizes ISPs to develop spam-blocking criteria and to employ

---

[67] *See* § 3.4, Commission of the European Communities, *Communication on Unsolicited Commercial Communications or "Spam,"* COM(2004)28 final at 17-18 (Jan. 22, 2004), *available at* http://europa.eu.int/information_society/topics/ecomm/useful_information/library/communic_reports/index_en.htm; *see also* Commission of the European Communities, *Proposal on Cooperation Between National Authorities Responsible for the Enforcement of Consumer Protection Laws*, COM(2003)443 final (July 18, 2003), *available at* http://europa.eu.int/comm/consumers/prot_rules/admin_coop/443_220240_en.pdf&e=10431.

[68] Mylene Mangalindan, *Spam Queen for Bulk E-mailer*, WALL STREET JOURNAL, Nov. 13, 2002, at A1 (noting the comments of an Internet direct marketer that she could make a profit if she got as few as 100 responses for every 100 million messages sent).

[69] § 16(9), *Spam Act 2003*.

[70] § 5.17, *Proposed Legislative Framework for the Control of E-mail Spam* (Singapore).

means to actualize these criteria though providers must notify clients of these practices in their subscriber contracts.[71] Such provisions provide legal cover for ISPs who must manage the flood of spam messages they receive. Measures adopted by ISPs, such as filtering, authentication, or port-blocking, will inevitably block some legitimate traffic while also missing some spam. ISPs may be wary of adopting such measures for fear of facing litigation by unhappy users or advertisers whose messages are blocked or mistakenly identified as spam. These provisions may be helpful if intermediaries such as ISPs are fearful of adopting spam controls due to concerns about legal liability.

It may be important to assess the level of competition in the ISP market to ensure that users have meaningful choice in which provider (and, concomitantly, which level of spam filtering) they select, as ISPs are likely to offer different levels of filtering services to meet the different preferences of users. If a state has only a single Internet service provider – for example, an incumbent monopoly telecommunications company – legislators may need to include more tailored provisions to protect users' ability to protest unwarranted blocking rather than blanket immunity from liability. Moreover, in a system without spam regulation, ISPs might choose to filter messages excessively to reduce their direct costs from spam. Since users are generally unaware of lost legitimate messages, pressures from consumer dissatisfaction from such measures could prove insufficient to drive competition in this area. Provisions relieving ISPs from liability for attempting to control spam are often linked to measures requiring or encouraging collaboration among and adoption of industry best practices by providers.

6) Permitted actors: **Common / Varying**

A key enforcement question is the question of enforcement: who is allowed to pursue a spammer for alleged violations of spam laws? There are five potential actors who could, individually or in combination, be tasked with enforcing such regulations:

[71] Art. 50-4, *Act on Promotion of Information and Communication and Communications Network Utilization and Information Protection of 2001* (as amended by Act No. 6797, Dec. 18, 2002).

- State entity (attorney general, justice ministry, data protection agency, specialized spam / communications agency, etc.)
- Service providers (ISPs, mail service providers, etc.)
- Individual users and Internet domain holders (account holders or computer owners who receive spam)
- "Bounty hunters" – private third-party enforcers who pursue violators to gain financial compensation or for personal reasons[72]
- Self-enforcement (policing by private parties, such as ISPs, through codes of conduct or agreements with individual users)

Allowing designated state actors, such as a national-level justice agency or data protection agency, to enforce relevant legislation is quite common.[73] Self-enforcement mechanisms, such as cooperative arrangements among ISPs, are also common and relatively uncontroversial. No state has yet established a formal bounty hunter program for enforcement. Some spam laws permit ISPs to bring suits to enforce spam provisions, either because they have suffered damages directly or on behalf of their users.[74] ISPs can be excellent enforcers because they must expend significant resources on combating spam and because they can function to aggregate the claims and harm suffered by their users. Allowing ISPs to seek statutory damages can help them become even more effective enforcers since it removes the difficulties of proving the exact amount of damages or harm suffered, which can be challenging to quantify in the electronic communication context.

One of the most common disputes over enforcement is whether to allow individual users who receive spam to pursue the spammer – a "private right of action." Countries such as the United States do not permit individual suits against spammers, believing that individuals have insufficient incentive to sue and that a series of lawsuits for small levels of harm would be inefficient. Moreover, plaintiffs' attorneys may pursue claims against legitimate marketers who make inadvertent errors rather than against more egregious violations since legitimate entities are easily located and have sufficient resources to satisfy a judgment. Other states, such as Malta and Argentina, allow private individuals to pursue violations of applicable legislation in court.[75] Individual rights of action may be particularly important if framed as part of a regime of data protection where the revelation or misuse of personally identifiable information is seen as causing harm to citizens regardless of the pecuniary effects of such violations. On their own, individual users may well lack sufficient incentives to enforce spam laws effectively. However, regulators who wish to include individual enforcement rights in their laws can bolster efficacy by providing for statutory damages, allowing users to aggregate claims through methods such as class

[72] The "bounty hunter" approach was prominently suggested by Stanford Law School professor Lawrence Lessig. *See* Lawrence Lessig, *Code Breaking: A Bounty on Spammers*, CIO INSIGHT, *at* http://www.cioinsight.com/article2/0,1397,1454839,00.asp (Sept. 16, 2002). The United States Federal Trade Commission evaluated, and essentially rejected, this proposal, finding that government employees and volunteer spam-fighting groups made the bounty hunter concept unnecessary. *See* Federal Trade Commission, *A CAN-SPAM Informant Reward System: A Report to Congress* 20-21, *available at* http://www.ftc.gov/reports/rewardsys/040916rewardsysrpt.pdf (September 2004).

[73] *See, e.g.,* Ministry of Public Management, Home Affairs, Posts and Telecommunications, *MPHPT appoints designated body to determine appropriateness of sending specified email messages*, July 10, 2002, *at* http://www.soumu.go.jp/joho_tsusin/eng/Releases/Telecommunications/news020710_3.html (Japan); §§ 34, 36, *Personal Data Protection Act*, RT I 2003, 25, 158, Feb. 12, 2003, *available at* http://www.legaltext.ee/text/en/X70030.htm (establishing the Data Protection Department of the Ministry of Internal Affairs in Estonia).

[74] *See, e.g.,* § 5.32, InfoComm Development Authority of Singapore – Attorney General's Chambers of Singapore, *Proposed Legislative Framework for the Control of E-mail Spam* (proposing to allow ISPs to sue if they suffer harm or damage from spam); 15 U.S.C. § 7706(g)(1) (2004) (United States) (allowing Internet access services to sue for an injunction or damages if "adversely affected" by certain violations of the CAN SPAM Act).

[75] §§ 33(b), 34, Law No. 25326 (Argentina); Art. 12(1), *Processing of Personal Data (Electronic Communications Sector) Regulations, 2003* (under the Data Protection Act (CAP. 440), L.N. 16 of 2003) (Malta).

actions, and providing streamlined procedures for complaints to enforcement agencies or for administrative procedures to pursue alleged violations. Thus, the decision to include or exclude individual user enforcement in spam laws should be treated as a component of an overall scheme to implement effective enforcement at the lowest cost for that level of enforcement; such enforcement rights are neither economically infeasible nor absolutely required for spam laws to work.

Overall, existing spam regimes demonstrate important variation in the entities that are vested with enforcement power, the resources at their disposal, and the extent to which these regulators are empowered to do their job against very long odds. A harmonization or model law effort must account for these different approaches and the views of efficiency and effectiveness that underlie them.

7) Cooperation / coordination among relevant regulatory / enforcement agencies: **Common / Varying**

As noted in the jurisdiction section above, spam implicates multiple regulatory regimes in most instances, from deceptive advertising to computer misuse to data privacy. Regulators must recognize that spam laws operate as one part of a system of controls that govern advertising through electronic communications. Each state or regulatory system must assess the various legal mechanisms that apply to spam and the overlap among these that occurs, both in formal terms and in enforcement. Lithuania controls advertising (including through electronic mail) using multiple regulatory bodies, including the National Board for Consumer Protection, local executive branches of government, and the state agency tasked with protecting cultural properties.[76] Lithuania's Law on Advertising clearly divides responsibility for areas of competence and enforcement among these bodies.[77] The state's Law on Electronic Communications creates a Communications Regulatory Authority with primary responsibility for spam and related communications issues. Lithuania specifies the interaction between the CRA and entities such as the National Consumer Rights Protection Board and the State Data Protection Inspectorate.[78] This type of explicit division of authority and responsibility can reduce uncertainty, thereby offering the potential for more efficient, effective enforcement.

Spam laws should seek to clarify and coordinate responsibility for various aspects of the problem. They should encourage communication and joint efforts among responsible entities both horizontally (for example, among national bodies charged with data protection, consumer protection, etc.) and vertically (for example, at different levels of government). Regulations could, for example, establish working groups or coordinating bodies that bring together relevant officials to improve collaboration and reduce redundancy. A model law could, and likely should, include provisions that mandate regulatory entities to form information-sharing and co-enforcement partnerships. While the precise details of such coordination will vary with the individual system at issue, including such provisions in a model law would focus attention on the need for this type of cooperation and would establish expectations that it would occur.

[76] Arts. 13, 17, *Law on Advertising*, No. VIII-1871, July 18, 2000, *available at* http://www3.lrs.lt/cgi-bin/preps2?Condition1=117415&Condition2=.
[77] Arts. 17-19, 23, *Law on Advertising*.
[78] Arts. 6, 8-9, 12, *Law on Electronic Communications*, No. IX-2135, Apr. 15, 2004, *available at* http://www3.lrs.lt/cgi-bin/preps2?Condition1=242679&Condition2=.

8) Penalties for Violations: **Common / Varying**

The penalties for violating the dictates of regulations on spam generally fall under one of three categories: administrative penalties imposed by an enforcement entity, civil damages (actual or statutory) imposed by an adjudicating court, or criminal penalties imposed by a court in a criminal prosecution. Many legal regimes mix multiple types of penalties, typically imposing administrative fines for less serious violations and reserving criminal prosecution for more egregious or harmful offenses. Mexico provides for fines under its Consumer Protection law for violations. Fines are enhanced for repeat or multiple violations, and violators may face a short period of incarceration in extreme cases.[79] South Korea creates civil liability of up to ten million Won for most violations of its spam laws and also provides criminal penalties for spammers who send advertisements for adult materials to minors or who use prohibited technological tools.[80] Provisions specifying enhanced penalties for repeat violators, and allowing entities harmed by spam to seek injunctive relief to mitigate or prevent future harm, are common.

The level and type of penalties imposed in spam laws must reflect both a subjective judgment about the relative gravity of the harm in question and a more objective calculus about how to enforce effectively the relevant law. For example, criminal penalties may be used to punish particularly grave harms, such as those involving victims who are minors or to create deterrence where identifying the violator is difficult or rare. How penalties are structured may also reflect challenges in enforcement. For example, spam laws may provide for statutory damages for violations due to the difficulties of quantifying the harm caused by a spam message or messages. Since this problem of proof can deter enforcement by allowing violators to evade penalties when evidence of quantifiable harm is lacking, and by increasing the costs and uncertainty of recovery for enforcers, statutory damages encourage enforcement and increase deterrence. Some jurisdictions, such as the United States, allow recovery of either statutory or actual damages at the enforcer's election.[81]

Administrative penalties may be particularly useful as spam sanctions. Administrative agencies often use less formal and more rapid adjudication measures than court systems do; this reduction in the cost of enforcement can help improve compliance (assuming it is not offset by a corresponding increase in error rates in decision making). In addition, an agency with scope limited to data protection or consumer protection issues may be more focused and better equipped to deal with a problem like spam than an entity with broad law enforcement responsibilities.

F. Points of Convergence / Consensus

Our analysis of the typology of existing spam laws reveals that there are a number of elements upon which there is strong consensus. Current efforts in these zones show both a strong tendency to include these elements as part of a legislative scheme to curtail spam and a relatively uniform approach to drafting and implementing these provisions. These elements should be strongly considered for inclusion in a model spam law; they are likely to be uncontroversial and are more likely to be effective because of the general accordance of views on them. We posit that there are seven elements on which there is convergence in legislative provisions:

- **Content:** Focus on commercial / transactional messages, including advertising
- **Disclosure:** Require the message to identify the sender and the advertiser

[79] Arts. 126-129, *Federal Law for Consumer Protection*.
[80] Arts. 64 (criminal penalties), 65-2, 67, *Act on Promotion of Information and Communication and Communications Network Utilization and Information Protection of 2001* (as amended by Act No. 6797, Dec. 18, 2002).
[81] 15 U.S.C. § 7706(f)(3) (2004) (imposing a $2 million US cap on statutory damages for most violations).

- **Truthfulness:** Prohibit fraudulent or misleading content (including subject lines), and ban concealing or altering the routing path of the message
- **Addresses:** Ban collection or generation of recipient addresses through address harvesting or dictionary attacks
- **Existing Relationship:** Permit a sender to contact a recipient if the two parties have an established relationship, such as a prior transaction involving goods related to the subject of the message
- **Refusal:** Mandate that recipients have the ability to unsubscribe from future communications from a sender, and that senders both respect this request and not exchange the addresses of users who have opted out with others (except as needed to fulfill the request)
- **Liability:** Employ a graduated mixture of civil and criminal penalties

G. Points of Divergence / Difference

There are also key areas of disagreement that will challenge efforts at harmonization or the creation of a model spam law. These differences often derive from diverging views on what constitutes permissible communication or the most efficient way to achieve enforcement. A harmonization or model law approach must grapple openly and, at the outset, with these challenges, in particular by attempting to elucidate their underlying assumptions, values, and beliefs. This is necessary because each of these points of divergence is critical to the success of legislation designed to control spam. We find five such points and explain briefly why each one is important:

- **Prior Consent:** Prior consent determines whether a sender must obtain prior permission from a recipient before directing a message to that user, and thereby defines whether an unsolicited communication is permitted or a violation. Variation in opt-in versus opt-out approaches makes cross-border efforts hard since an offense in an opt-in regime may be legal in an opt-out one.
- **Enforcement:** Enforcement sets who is permitted to recover for or prosecute violations of the law and, in particular, whether private entities such as ISPs and spam recipients may recover damages. This issue is important as it determines who must devote resources to pursuing violations and also because a party with a cause of action in one regime may seek to pursue a violator in another system, only to discover that they have no recourse there.
- **Labeling:** Labeling creates requirements for what characters or words a sender must include to identify a message as spam. Greater consensus in labeling requirements improves the ability of users and providers to filter spam; divergence makes compliance harder for senders.
- **Applications:** Applications establish the scope of spam laws across electronic (and potentially other) media. Regimes that employ a more application-agnostic approach will not need to update their laws as new technologies, such as Web logs, become established and confront the problem of spam. Differences in approach in this zone can create havens for spammers who can re-locate to jurisdictions that do not penalize their behavior for a new medium, at least until that system updates its laws.
- **Jurisdiction:** Jurisdiction defines the reach of a system's spam laws. Variations between broad and narrow approaches can create conflicts between sovereigns over who has authority to control an alleged violator's behavior, efforts to "forum-shop" by enforcers and plaintiffs, and uncertainty in senders about whose rules apply.

H. Conclusion

Analyzing the elements that form existing spam laws provides a set of building blocks for a model law or harmonization effort. By identifying whether an element is common or rare, and whether it is implemented in a uniform or varying fashion when found, we uncover both areas of consensus and zones

of divergence in legal approaches to spam. Efforts to align spam laws must leverage the accordance of views on the former and seek to understand and work through the differences in the latter in order to succeed.

IV. Other Modes of Control: Potential Dependencies for Spam Laws

A. Technical Measures

To succeed in controlling spam, regulatory efforts through legislation and rulemaking must be accompanied by – or at least coordinated with – technological reform measures that reduce the incidence of these unwanted messages while minimizing the impact on legitimate messages. These technical methods – some currently at the proposal or experimental stage and others in widespread usage – fall roughly into four categories: filters, cost-shifting, authentication, and security.

1) Filters

Filtering attempts to detect and block or quarantine spam messages. Filters can be installed at many layers of the network, for instance by e-mail service providers, Internet service providers, and individual users. Filters search messages for characteristics that indicate spam, such as a fictitious domain in the message's return address or the presence of keywords such as "Viagra", or close variants such as "Vi*gra," in its body. More sophisticated filters employ techniques such as Bayesian statistical analysis that use probabilistic assessment of words in a message and that are capable of refinement with increased accuracy over time.[82] Filtering can prevent end users from even seeing spam messages, and by reducing the risk that they (or their children) might be exposed to offensive content such as graphic advertisements for pornography. Filters are widely used both by ISPs and by individuals at the client level to reduce e-mail spam. While most filters are produced by private companies or developers, spam regulators may be authorized to contribute to or to support such tools.[83] Moreover, some states provide authority for enforcement agencies to order intermediaries to filter or block spammers.[84]

[82] *See generally* Paul Graham, *A Plan for Spam*, *at* http://www.paulgraham.com/spam.html (Aug. 2002) (describing a Bayesian software filter's code and underlying analysis). Bayesian analysis offers the capability to refine a filter's analysis through classification of messages by users or administrators.

[83] See, e.g., §§ 113(3)(q)-(t), *Telecommunications Act 1997* (Australia), *available at* http://scaleplus.law.gov.au/html/pasteact/2/3021/0/PA001510.htm; § 130, *Personal Data Protection Code*, Legislative Decree no. 196 of June 30, 2003, *available at* http://www.garanteprivacy.it/garante/document?ID=727068 (English-language version) (Italy).

[84] *See, e.g.,* Arts. 8, 39, Law 34/2002, July 11, 2002 (as modified by Law 32/2003) (Spain); § 130, *Personal Data Protection Code*, Legislative Decree no. 196 of June 30, 2003 (Italy).

a) Blacklists / Whitelists

Filters can be augmented using two additional tools: "blacklists" and "whitelists". Blacklists compile data about known spam sources and senders.[85] This enables service providers to scrutinize or block e-mail traffic from these sources. Blacklists are generally compiled and maintained by private companies or organizations. Though blacklists can be valuable in blocking defined sources of spam, their use implicates questions about standards for being added to and removed from a list, the speed of updates, and the power such lists confer on the compiler. In addition, spammers have begun to adopt new techniques, such as routing messages through ISP servers that reduce blacklists' effectiveness.[86]

Whitelists perform the opposite role as they validate certain senders as sources of legitimate messages. Therefore, messages from these senders either bypass filtering entirely or are scrutinized at a much reduced level. Simple whitelist techniques, for example, allow senders listed in a user's address book to bypass filters installed by that end user. More advanced methods, such as "bonded sender" or "payment at risk" programs, incorporate monetary guarantees by senders. Payment at risk penalizes a sender financially if a message is spam or if the recipient is dissatisfied with it.[87] Bonded sender programs require senders to post a monetary guarantee of their e-mail advertising before they are permitted to bypass spam filters.[88] Whitelists simplify filtering by classifying certain messages as "low risk," meaning that it's highly unlikely they are spam. However, whitelists impose costs on senders that may have negative distributional consequences and require the participation of filtering entities to be effective. Whitelists are also ineffective if a message falsely purports to be sent by a sender in the whitelist or is sent from a hijacked computer in the whitelist.

b) Drawbacks

While filtering is an important tool in addressing spam, it suffers from three primary drawbacks: overblocking, underblocking, and reduced control. Overblocking by filters removes legitimate messages as well as spam. The level of overblocking depends both on the filter used and its implementation. A study by e-mail marketing firm Return Path found that seventeen percent of permission-based messages (whose recipients consent in advance to receive the e-mail) were blocked by spam filters.[89] This over-inclusiveness can also occur when users attempt to send messages if their service provider implements outbound spam filtering.[90] Overblocking is harmful because it prevents recipients from accessing (or sending) desired, legitimate messages and because it undermines their confidence in the reliability of e-mail as a communications medium.

Underblocking occurs when filters fail to detect or to remove messages that are spam. This under-inclusiveness results both from the arms race between spammers and filters – for example, spammers

[85] *See, e.g.,* The Spamhaus Project, *The Spamhaus Block List*, *at* http://www.spamhaus.org/sbl/index.lasso (last visited June 10, 2005); Spamcop.net, *Blocking List*, *at* http://www.spamcop.net/bl.shtml (last visited June 10, 2005).
[86] *See* Jonathan Krim, *Spammers' New Strategy*, WASHINGTON POST, Feb. 4, 2005, at E1 (quoting the director of anti-spam operations at AOL as stating that 95% of spam directed at AOL comes from ISP servers, which "strikes at the heart of the blacklist system").
[87] *See* Tim Weber, *Gates forecasts victory over spam*, BBC NEWS, *at* http://news.bbc.co.uk/2/hi/business/3426367.stm (Jan. 24, 2004) (discussing Microsoft chairman Bill Gates's proposal for "payment at risk").
[88] *See* Bonded Sender Program, *Frequently Asked Questions – General Questions*, *at* http://www.bondedsender.com/faqs/general.html#what_is_bsp.
[89] Hiawatha Bray, *As war on spam heats up, many valid e-mails are getting lost*, BOSTON GLOBE, Feb. 18, 2004, at A14 (stating that overblocking occurs more often with smaller ISPs and organizations with less skill in configuring filters).
[90] *See, e.g.,* Paul Festa, *Comcast goofs in Russian spam blockade*, CNET NEWS.COM, *at* http://news.com.com/2102-1038_3-5168643.html (Mar. 2, 2004).

have begun including unusual but innocuous words in messages to evade Bayesian filters – and from the difficulties inherent in analyzing the content and intent of e-mail.[91] Underblocking demonstrates that technical methods are only a partial solution to spam.

Finally, spam filters implicate important questions of control over receiving and sending content.[92] Filters implemented at the service provider level decrease the control that end users have over what types of messages they receive. For example, an individual user might prefer to receive certain unsolicited messages, such as messages advertising credit card offers, and such messages may be blocked as spam from his ISP. Alternately, a user might decide the risk of not receiving even a single incorrectly blocked message is unacceptable. Conversely, filtering implemented by end users may be updated less frequently and configured less skillfully if users are not technologically savvy. This is particularly important regarding spam that contains viruses, worms, or bots.

2) Cost-Shifting

Cost-shifting proposals seek to reduce the volume of spam by increasing the sender's costs, either in money or in computing time, to transmit each message.[93] The goal is to alter the unusual economics of spam, in which the sender incurs almost no cost to send messages while the costs to transport the message, store it, and delete it are borne by the recipient and third parties such as ISPs. In addition, senders can often transmit a single message that is delivered to many recipients. Thus, since the advertising item itself does not need to be printed and distributed as a separate piece for each recipient, sending large numbers of solicitations does not incur increasing costs. The result is that fractional response rates that would be a disaster in traditional direct marketing become profitable on the Internet.

a) E-stamp (Electronic Postage)

E-stamp solutions propose to modify the electronic mail infrastructure to either allow or require a monetary payment for each message sent. Even a tiny increase in the costs of sending an individual message would make mass mailings of tens of millions of messages economically unfeasible. Commercial mass marketers accustomed to traditional response rates in other media should not be deterred by a small charge to send marketing material. In addition, many E-stamp proposals provide a base daily level of free messages (such as a hundred per day at no charge) to individual users, so few senders would incur any additional cost.

Unfortunately, E-stamp proposals suffer from a number of drawbacks. As many observers have noted, such an increase in cost would prove crippling to many developing nations that are in the early stages of adopting new information and communications technologies infrastructures. All of these proposals not only require major changes to the existing electronic mail infrastructure, but also penalize everyone who sends e-mail, not just spammers. Since any additional cost imposed on each message cost must be a fixed, relatively small amount, this form of cost-shifting is unlikely to deter the most harmful forms of spam -- those seeking to defraud the recipient -- that offer the sender relatively large rewards. In addition,

[91] *See generally* CipherTrust, *How Spammers Fool Spam Filters – And How to Stop Them*, *at* http://www.ciphertrust.com/resources/articles/articles/foolspam.php (last visited June 10, 2005).
[92] *See generally* David R. Johnson, Susan P. Crawford, & John G. Palfrey, Jr., *The Accountable Internet: Peer Production of Internet Governance*, 9 VA. J. L. & TECH. 9, ¶ 44, *available at* http://www.vjolt.net/vol9/issue3/v9i3_a09-Palfrey.pdf.
[93] *See, e.g.*, Paul Boutin, *Can E-Mail Be Saved?*, INFOWORLD.COM, Apr. 19, 2004, at 40 (describing the "Penny Back" project which requires a computer sending e-mail to compute a time intensive value as a cost before the recipient will accept the message and noting that the scheme could be circumvented by the use of zombie drones and the difficulty of getting foreign countries to participate); Randall Stross, *How to Stop Junk E-Mail: Charge for the Stamp*, N.Y. TIMES, Feb. 13, 2005, at BU5 (concluding that payment of money or computation time is the solution to spam).

while a penny per message charge may be negligible to a large developed-country corporation, it may be a significant amount of money in the developing world (in which case a pay-to-send system could worsen the digital divide). Developing and deploying the infrastructure for every mail server and client in the world to handle micro-payments in world currency appears daunting at best and impossible in any near-term time frame. Finally, even at small per-message amounts, the huge amount of daily e-mail traffic implicates dollar amounts that create a sizeable opportunity for fraud and electronic theft from any system of cash E-postage.

b) Computing Solutions

As an alternative to requiring a cash payment for each message, several anti-spam proposals would require the sending computer to compute a complicated numerical puzzle and return the correct answer to the recipient before the recipient would accept the message. This creates a small delay in sending each message. While invisible to most users, such methods would make it impossible for a spammer to send tens or hundreds of millions of messages a day from a few computers connected to the Internet. Because computing solutions do not involve money transfers, the issues of currency conversion, fraud, and relative value plaguing E-stamp solutions are minimized.

However, computing solutions still require major changes to the e-mail infrastructure and burden all senders, not just undesirable ones. Much of the value of e-mail derives from its low cost. Many legitimate senders, including businesses, government agencies, private organizations, and independent newsletter authors, send large quantities of electronic mail. Much of this traffic is not income-generating but informational; for example, the low cost of sending e-mail has enabled incremental package tracking, frequent government informational updates, and a host of special-interest electronic newsletters from non-commercial and non-profit entities. Changing the economics of bulk e-mail could drastically curtail the free flow of information that characterizes the Internet. Finally, much of the current spam problem originates from computers that have been hijacked by spammers.[94] If spammers can employ other users' resources to transmit messages, computing cost solutions are unlikely to deter unwanted messages while placing a severe burden on legitimate senders.

3) Authentication

Any legal solution to regulating spam, even one well-harmonized among different regimes, is challenged by the difficulty of holding violators accountable. The Simple Mail Transport Protocol (SMTP) used to transmit Internet e-mail does not authenticate senders, allowing violators of messaging regulations to hide their identities behind false header information, hijacked zombie drones, open relays, and proxies.[95] The result is that laws regulating commercial message content or form often constrain legitimate businesses but are ignored by illegal or fringe operators. A number of methods of improving accountability through sender authentication have been proposed, but none has been universally adopted yet.

Authentication seeks to allow a recipient to verify who sent a message. Authenticated e-mail offers several benefits. First, the recipient can decide, either manually or automatically, to accept the message based on the actual sender's identity. Much spam is currently "spoofed" by listing a false or non-existent sender. Having authenticated sender information allows filters and whitelists to operate more efficiently and accurately, and makes evading blacklists of known violators more difficult. Authentication also makes enforcement easier and cheaper. If senders cannot hide their identities, law enforcement need not

[94] *See* Tom Zeller, Jr., *Law Barring Junk E-Mail Allows a Flood Instead*, N.Y. TIMES, Feb. 1, 2005, at A1 (claiming millions of hijacked computers provide a zombie network to send spam);

[95] *See, e.g.*, Paul Boutin, *Ending E-Mail Forgery*, INFOWORLD, Apr. 4, 2004, at 52 (noting a general agreement that the basic problem in stopping spam is a lack of authentication for sender address in SMTP).

expend significant resources tracking down and proving who violators are. Finally, authentication may deter spammers from violations since they can expect their identities to be revealed.

a) End-to-End Solutions

Cryptographic solutions to combat spam also appear promising. Yahoo!'s DomainKeys proposal, Cisco's Identified Internet Mail (IIM) method, and Bounce Address Tag Validation (BATV) all attempt to prevent falsification of sender's addresses by requiring a message's originator to encrypt at least part of the message with a private cryptographic key known only to the legitimate holder of the sender's address or domain. The recipient then uses a publicly-available cryptographic key (provided by the holder of the domain or address claimed as the sender) to decrypt the message. If the message can be decrypted, it originated with someone with access to the private key. Thus, the recipient can treat the message as legitimate. These proposals currently only authenticate the sender's domain, but could theoretically be extended to cover individual addresses.

These methods generally propose to distribute the public key information necessary to decrypt a received message through the Domain Name Server (DNS) system currently used to map domain names to Internet Protocol (IP) addresses. The proposals simplify implementation by allowing individual domain owners to manage their cryptographic keys, avoiding the need for a single overarching key authority. The current DNS system can store and retrieve cryptographic keys with no modification. However, each end-to-end scheme requires significant changes to both e-mail clients sending messages and the servers attempting to authenticate them. Since there are over thirty million Internet domains, any change to how e-mail works will certainly be adopted gradually, and many servers may never upgrade. Therefore, any authentication scheme will have to deal indefinitely with a significant volume of legitimate e-mail which does not support authentication.

b) Last-Hop Solutions

Microsoft and developer Meng Wong independently proposed authentication solutions that authenticate only the most recent connection that transferred a message, rather than authenticating the entire chain of transfer from the message's originator to the recipient. These proposals have been merged into a single proposal, "Sender ID for E-mail." Sender ID only authenticates the domain of the most recent message transferor; unlike end-to-end solutions, it cannot be extended to individual senders.

The primary advantage to last-hop solutions is that they do not require modification of the sender's mail server. Thus, domains can be made compatible with Sender ID even if their mail server cannot be modified. A domain can implement Sender ID for its outgoing messages with little time or effort by adding a new Sender Policy Framework (SPF) record to its DNS entry. Although Sender ID does not require modification of the sending server, the receiving mail server, or the recipient's mail client, must be modified to support Sender ID to authenticate the message. Thus, a last-hop solution provides an immediate method of supplying authentication information for messages that can be easily adopted by every sender. Only recipients who want to verify senders' information need modify their existing e-mail software.

c) Interaction of Legal Regimes and Authentication

Since enforcement of spam regulations requires identifying violators, legal systems have an interest in encouraging or mandating authentication. For example, the Federal Trade Commission, the agency responsible for enforcing the federal U.S. anti-spam act, has indicated that it may mandate an

authentication protocol if market forces fail to supply a consensus choice.[96] However, unless all systems adopt a compatible method, authentication is unlikely to simplify the difficult task of cross-jurisdictional enforcement. In addition, the economic costs and physical impossibility of universal adoption limit the extent to which states can mandate, rather than encourage, authentication. We believe it is worthwhile for states to discuss authentication technologies to increase the probability that a single technology, amenable to the varying needs of different systems, will be adopted.

d) Limitations of Authentication

Neither last-hop nor end-to-end authentication can distinguish legitimate messages from illegal messages sent by hijacked computers. If an authentication scheme is adopted that makes it impossible for messages to be sent anonymously, violators will increase efforts to compromise and use others' equipment to send their messages. States may need to create liability for third parties who do not take reasonable steps to prevent their equipment for being used for illegal purposes. For example, an ISP who failed to secure a mail server could be held liable if that server were used to send spam.

In addition, universal adoption of any authentication method is unlikely given the large number of mail servers worldwide. This may make mandated authentication impossible; thus, legal regimes may instead move to provide incentives to entities, such as service providers, who voluntarily adopt solutions that make identifying violators easier.

4) Security

Spam is intimately linked to computer and network security. Increasingly, spammers use a distributed mechanism to transmit messages from multiple sources. This method involves compromising the security of numerous computers with high-speed Internet access through viruses or worms that exploit flaws in operating systems or a user's failure to install and maintain firewall and anti-virus software. Once compromised, these "zombie" computers send messages on behalf of the spammer. This disguises the sender, evades ISP limits on the number of messages one source can transmit, and reduces the spammer's hardware and bandwidth costs. Zombies are estimated to produce seventy percent of spam currently.[97] Computer security company Symantec estimates that thirty thousand computers become zombies each day.[98] Groups of these zombie computers, known as "botnets," are sold or rented for malicious purposes ranging from denial of service attacks to mass transmissions of spam.[99] Thus, maintaining proper security – even for home computers – is vital to the success of efforts against spam.

Intermediaries such as ISPs and messaging service providers can, and do, take measures to improve security and to decrease the vulnerability of users and of networks. For example, Google's Gmail free e-mail service removes hyperlinks from messages that the service believes to be "phishing" attempts.[100] ISP Earthlink requires all e-mail messages to route through its mail servers to reduce the impact of zombie networks and mandates that users' e-mail programs submit passwords to transmit messages.[101] While these methods can reduce the burden of spam, it is important to recognize that end users must also

[96] *See* U.S. Federal Trade Commission, *National Do Not Email Registry: A Report To Congress* 36 (2004), *at* http://www.ftc.gov/reports/dneregistry/report.pdf.
[97] *See, e.g.,* Mello Jr., *CAN-SPAM Compliance Hits New High of 6 Percent* (noting MX Logic found that zombie networks accounted for 69% of spam in November 2004).
[98] *See* Krim, *E-Mail Authentication Will Not End Spam, Panelists Say*.
[99] *See* Ryan Naraine, *Botnet Hunters Search for "Command and Control" Servers*, eWEEK, June 17, 2005, *at* http://www.eweek.com/article2/0,1759,1829347,00.asp.
[100] *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.
[101] *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.

exercise significant responsibility for maintaining a secure, safe computing environment. Users who do not update virus software and operating systems automatically or regularly, or who download programs that contain "malware" and "spyware" that compromise their computer, pose a risk not only to themselves but to other users worldwide. Thus, security measures must operate in conjunction with user education campaigns (as discussed at Section C *infra*).

B. Enforcement Efforts

Enforcement is the greatest determinant of success in virtually every legal regime, but certainly so in the case of legal regulation of spam. Laws backed by aggressive, skilled, and sustained enforcement are necessary if any such legal regime is to generate meaningful results. Enforcement challenges legal regimes in a number of ways, including:

- The need to sustain effort over time
- Resource demands for scarce funds, personnel, and official emphasis
- Coordination among enforcers vertically and horizontally within a system
- Coordination across national and jurisdictional boundaries
- Technological difficulties tracking, identifying, and proving the sender or responsible party for spam
- The need for significant, ongoing cooperation from private parties such as ISPs, end users, domain owners, and others

Enforcement efforts exist outside the drafting of regulation, but these moves can be assisted by spam laws. For example, harmonization of provisions to align with those of other systems can ease the difficulties in pursuing violators across borders. Clearly delineated lines of responsibility can avoid contests for control and authority among enforcement entities. Moreover, express authorization for multi-state efforts can confer legitimacy upon them and can create mechanisms by which this type of enforcement takes place.

We close with two critical points about effective enforcement. First, collaborative efforts must include not only formal, legal enforcers, such as data protection agencies and communications authorities, but also entities that implement spam regulation through other means, such as service providers and Internet access providers. Sharing of best practices and information on sources of spam, spam-friendly hosting services, and compromised computers can greatly enhance the effectiveness of legal regimes that govern spam.[102] Legal enforcers must treat these other parties in the spam battle with respect and must engage them fully in an on-going fashion.

Second, enforcement across borders for spam control is paramount if any legal anti-spam efforts are to be effective. Early efforts to coordinate anti-spam enforcement appear promising, as the United States FTC representatives and others remarked at the ITU's 2004 Workshop on combating spam. But underlying differences in legal regimes, unrelated to the specifics of a spam law, and the realities of other priorities cut against the likelihood of effective, widespread international coordination of anti-spam enforcement.

C. User Education

Users, who are often victims of spam, are also a large component of the problem for two reasons. First, they read spam messages and purchase items advertised through them. The Business Software Alliance

[102] *See, e.g.,* Riva Richmond, *Firms Join Forces Against Hackers*, THE WALL STREET JOURNAL, Mar. 28, 2005, at B4 (describing how 18 telecommunications service providers will share information on hackers and network attacks).

found, for example, that twenty two percent of British consumers purchased software through spam.[103] Rates for the other five countries surveyed by BSA were similar. Spam persists because it is a profitable undertaking. If consumers did not make purchasing decisions in reaction to these communications, the messages would not continue (though phishing might well persist). Spammers will not pursue unprofitable methods, even when those methods are low-cost. The challenge is that spam offers an easy means to purchase items not otherwise lawfully available (such as illicit drugs) or not available as cheaply (such as illegally copied software). In this sense, spam is simply advertising for illegal goods and it persists along with the demand for those goods.

Second, users help provide resources for spammers by failing to maintain adequate computer security. As noted above, computer users who do not install and update protective measures such as firewalls, anti-virus programs, and spyware detection software enable spammers to make use of their computers and Internet connections. While a combination of default settings, such as providing a firewall as part of the device that connects a user to a broadband connection, and automated updates, such as weekly downloads of the latest virus definitions, can reduce this problem, users ultimately have the largest share of control over their computing environment.

Accordingly, user education is a necessary, ongoing, and only partly successful component of an effective legal regime to control spam. New users constantly move onto the Internet and must be taught to recognize and defeat tactics considered passé by experienced regulators and technical personnel. Moreover, education is always a partial success because users lack incentives to maintain perfect security. First, consumers do not gain the full benefit of measures they take to protect their computers; the reduction in spam volume they see bears little relationship to these actions. Second, many users will agree to host programs, such as adware, on their computer in exchange for free use of programs such as screensavers or peer-to-peer software. Thus, at best, user education will limit or contain this segment of the problem, but cannot realistically solve it.

[103] 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.

V. Initial Recommendations

Though legal reform alone will not end spam, it is worthwhile for countries to align their legal regulations regarding spam to the degree possible and to collaborate on anti-spam enforcement. We emphasize that each state or regulatory system must create a response to spam that accords with its priorities, its existing regulations for advertising, and its technical infrastructure. With this baseline assumption, though, congruence in laws increases the opportunity to combat spam's problems effectively and decreases the challenges inherent in the cross-border nature of electronic advertising. Accordingly, we make some tentative recommendations for regulators considering a model spam law or, indeed, any spam legislation concordant with our analysis of the four key questions in Part II.

A. Defining Prohibited Content

Existing laws governing spam show considerable unity in defining the content they proscribe, despite the thorny challenge of widely divergent views about what constitutes prohibited expression. Anti-spam laws around the world concentrate on content with a commercial, for-profit purpose. This focus recognizes both the financial incentives in commercial messages that drive their proliferation and also concerns about suppressing (often protected) dialogue on issues such as politics, religion, and culture. They also generally prohibit communications that seek to defraud or mislead the recipient, that conceal the identity of the sender or the advertiser on whose behalf the message is transmitted, or that disguise information about the path that the message took in reaching a user. There is variation in whether laws apply only to one specific application (such as e-mail) or to on-line communication more generally. We believe that regulating communications more generally economizes regulatory effort and provides a framework for controlling spam on emerging applications such as Voice over Internet Protocol (VoIP) (known as "SPIT" (Spam over Internet Telephony)), in blog formats, such as Really Simple Syndication (RSS) feeds, in Wikis, and on mobile devices.

A review of existing anti-spam laws suggests the following likely elements in a model law:

- Focus primarily on commercial content
- Ban fraudulent or misleading messages
- Prohibit concealing or falsifying a message's sender, advertiser, or routing information
- Draft regulations covering Internet communication generally rather than specifying applications (such as e-mail)

B. Setting Default Rules for Contacting Recipients

There is considerable divergence in the default rules that different legal structures establish for contacting recipients. The greatest difference is between opt-in and opt-out approaches. The core question is whether it is lawful to contact a recipient who has not previously consented to such communication (Nearly all regimes make it unlawful to contact recipients who have indicated to a sender that they do not wish to receive messages.) Given that this default rule is at the core of spam regulation in most systems and that there are a significant number of regimes in each camp, the clear message is that any effort to draft a model law must squarely face this challenge.

Labeling requirements also vary and differences may result in complications for any model law. Some systems require labels while others do not. Even among the former, the labels prescribed differ. This can make compliance difficult for legitimate advertisers who may have difficulty determining where a recipient resides and, thus, which labeling scheme applies. Thus, we believe that this is an area where

harmonization would be of significant benefit: senders could comply more easily with requirements and legal systems could help citizens identify and filter more messages if labeling schemes were aligned.

There is greater convergence in other default rules. Most regimes oblige senders to respect a recipient's decision to refuse future communications by unsubscribing, and most prohibit automated collection or generation of recipient addresses. Based upon the existing anti-spam laws, drafters of a model law ought to consider provisions that would:

- Require senders to provide recipients with a means to refuse, or unsubscribe from, future communications that is easy to use and inexpensive (preferably at no additional incremental cost)
- Require senders to respect unsubscribe requests and prohibit them from exchanging or selling addresses of recipients who unsubscribe
- Prohibit address harvesting and dictionary attacks, along with software tools specifically tailored to these purposes
- Seek to standardize labeling requirements

C. Harmonizing Existing Laws

Efforts to reconcile existing general laws (such as those that prohibit fraud, damage to the property of another, and so forth) with spam regulation must take place within each regional legal system. There is clearly a role for coordinating bodies to play in terms of assisting with this harmonization by making accessible the successful efforts of proximate states.

Meanwhile, there is a trend towards adopting spam-specific regulation rather than on solely applying general-purpose laws to electronic communications. We believe that spam poses unusual challenges to regulation given its cross-border context and unique financial structure. As such, regulators might consider efforts to:

- Adopt legal rules specific to spam
- Emphasize the need to align existing laws such as data protection and anti-fraud provisions with these new rules and to ensure that the theories underlying these regulations are coherent

D. Enforcing Rules

Enforcement is the most critical factor in the success of spam legislation. Harmonizing laws on spam, such as through a model law approach, can provide consistent responsibilities, penalties, and jurisdiction, but each legal system must carry the burden of enforcing these dictates.

Different regimes allocate responsibility for enforcing laws in varying ways. It is common to have one or more national-level bodies, such as a spam authority or telecommunications agency, as the chief enforcer. However, many systems have multiple enforcement bodies, including some that are involved only in a tertiary fashion (such as competition regulators). The way that these entities interact varies as well. It is obvious, though, that a clear division of responsibilities and a strong commitment to coordinated effort is vital.

A significant difference among systems is the role permitted to private actors in enforcement -- for example, whether entities affected by spam (such as end users or service providers) may bring suit against senders or the parties that advertise in the offending messages. While allowing private suits can save governmental resources and can permit these parties to recover economic harm from spam, there are

concerns that suits may target legitimate senders who make inadvertent errors rather than more egregious offenders (in part because legitimate senders are easier to identify and hale into court). This tension is one that a body working to harmonize laws or to draft a model law will be forced to confront.

Jurisdiction also varies. Some regimes have a circumscribed view of jurisdiction that requires that the sender be located within their borders for their rules to apply. Others take an expansive position, applying (at least in theory) their laws to any message that passes across a computer or network link inside their boundaries. We feel that harmonization of jurisdiction provisions could provide a number of benefits, including greater notice to senders as to which rules may apply, reduced potential for conflicts of law, and probably a greater willingness by different enforcers to cooperate.

The penalties for violating spam laws, while differing in specific levels, show greater similarity. Administrative fines imposed by regulatory agencies are common, as are criminal penalties for more egregious offenses (such as those involving minors or particularly sensitive content like pornography). Regimes that allow suit by private entities typically provide for civil damages either at a defined level or based on actual harm.

Based upon a review of existing law, we suggest that drafters consider provisions related to enforcement that would:

- Allocate primary responsibility for enforcing spam laws to a single entity within each state that is suitably funded and staff to pursue violations aggressively
- Establish explicit coordination, including coordination mechanisms, among entities with responsibility for enforcement (including, as appropriate, private actors such as ISPs)
- Create a graduated system of penalties, from administrative fines for minor offenses to criminal penalties for major or repeated violations
- Create secondary liability for entities that advertise products or services via spam to deter, to encourage advertisers to select reputable communications firms, and to set up incentives for advertisers to monitor the communications on their behalf
- Establish further Memoranda of Understanding between enforcement officials in multiple regions to facilitate enforcement cooperation

VI. Conclusion

The creation of a model spam law that emphasizes key components of such regulation and that maximizes areas of consensus with existing regimes offers the potential for benefits both for states that already regulate spam and for those that have not yet decided how to approach this problem. Increasing in broad terms the alignment and conformity of legal rules governing this type of coordination can improve enforcers' ability to operate, as spammers so often do, across jurisdictional boundaries. Greater similarity of provisions also provides clear notice to senders about acceptable, proscribed behaviors and reinforces social expectations about this conduct. Moreover, the creation of a model law can reduce the cost and challenges for legal systems that have not yet addressed spam; these regimes can enact and implement the law with confidence that it approaches a set of best practices in this area and that the new regulations will be compatible with a number of other states.

The creation and adoption of clear, thoughtfully crafted spam legislation merely provides the framework to attack the problem, though; it does not in itself provide a solution. At base, cleaning up spam is a question of resources, enforcement, and the effective integration of anti-spam laws with existing technology, market, and norms-based approaches. To combat spam effectively, regulators would need to be able to devote considerably more attention and effort than is currently directed toward this goal. Regulators must work closely with technical specialists to track down spammers and to gather proof of violations. They must coordinate closely with counterparts in other jurisdictions as spam will often cross borders on its path from sender to recipient. They must resolve questions of responsibility and competence within their own borders with regulators of related issues such as criminal fraud, data protection, personal privacy, and computer misuse. Without effective, concerted, sustained enforcement, any spam law is a dead letter: the difference between passing a spam law and implementing it on the ground is the difference between planning a journey and actually traveling it.