2004

Cracks in the Foundation: The New Internet Legislation's Hidden Threat to Privacy and Commerce

Joshua Fairfield
Indiana University School of Law

CRACKS IN THE FOUNDATION: The New Internet Legislation's Hidden Threat to Privacy and Commerce

Joshua A.T. Fairfield†

SYNOPSIS: *Scholarship to date has focused on the legal significance of the novelty of the Internet. This scholarship does not describe or predict actual Internet legislation. Instead of asking whether the Internet is so new as to merit new law, legislators and academics should re-evaluate the role of government in orchestrating collective action and change the relative weight of enforcement, deterrence, and incentives in Internet regulations.*

A perfect example of the need for this new approach is the recent CAN-SPAM Act of 2003, which was intended to protect personal privacy and legitimate businesses. However, the law threatens both of these interests, because it does not recognize either the limits of enforceability, or the enhanced possibilities for incentives offered by the decentralized architecture of the Internet.

I. INTRODUCTION

The debate over the usefulness of Internet regulation can be described as a conversation about the applicability of existing laws and rules to new situations.[1] The simplest trait of the Internet (and of like emerging communications systems) is its novelty.[2] Thus, the historical question of legal scholarship concerned with Internet regulation has been whether or not the Internet is sufficiently novel to merit passing new laws that take its specific technological characteristics into account.[3]

---

† Associate-in-Law, Columbia Law School. Many thanks to Professor Douglas Lichtman, of the University of Chicago, and Professor Eugene Kontorovich, of George Mason University, for comments and suggestions. Special thanks to Professor Timothy Jost of Washington and Lee for his ongoing advice and support, and to my father, John Fairfield, PhD., for his help with the technological details.

1. For an excellent non-legal treatment of the problem of applying words—which is, of course, all that statutes are—to novel situations, see SAUL A. KRIPKE, WITTGENSTEIN ON RULES AND PRIVATE LANGUAGE (1982).

2. A good synopsis of the early scholarly conversation about Internet regulation is offered by Timothy Wu, *When Law & the Internet First Met*, 3 GREEN BAG 2d 137 (2000).

3. *See generally id.*

However, to some degree, the novelty of instant, cheap, and repeatable communication has worn off, and legislatures have begun the practical work of hammering out solutions to Internet problems.[4] Discussions of whether the Internet is a novel medium, and ought to be governed by novel rules do not—alone—describe or predict the actual laws legislatures have produced. Legislatures have instead taken a pragmatic approach to regulation of the Internet, mixing statutory innovation with established jurisprudence. These laws rely on traditional understandings of jurisdiction—i.e., they rely on traditional conceptions of the reach and role of government, enforcement, and deterrence to stop prohibited conduct—but, conversely, adopt new substantive rules of law matched to specific technological features of the Internet.[5]

A pragmatic approach to Internet regulation is indeed desirable; legislatures should not be paralyzed in the face of new technology.[6] A traditional approach to jurisdiction, however—relying on the government to organize the response to wrongful acts, enforce laws prohibiting those acts, and secure penalties calculated to deter those acts—in fact can harm privacy and industry on the Internet.[7] Conversely, the selection of new rules that match specific technological features of the Internet creates increased risks of bad law both because technological features change rapidly, and because limits on use of technological functions often have unintended consequences.[8] Thus, instead of selecting novel rules enforced by traditional means, legislatures should do the exact opposite: enact traditional rules based on lessons already learned from other media, but re-evaluate the role

---

4. Congress has now had nearly a decade worth of experience in legislating Internet restrictions. The earliest broad-brush Internet regulations did not take the decentralized and cross-border nature of the Internet into account at all, and were struck down. *See* Reno v. ACLU, 521 U.S. 844, 874 (1997) (declaring the Communications Decency Act of 1996, which sought to prohibit the sending of offensive materials to minors, among other things, unconstitutional based in part on the inability of senders to determine who would receive the material). But the more recent Children's Internet Protection Act, Pub. L. No. 106-554 (2000)—which sought the same end by requiring libraries to install "censorware" on library computers—was upheld. United States v. Am. Library Ass'n, 539 U.S. 194, 214 (2003). Thus, roughly speaking, "client-side" censorship is permissible, as representing a decision by the recipient to refuse the communication, while "server-side" censorship is not. *See id.* at 211–12.

5. The clearest statement of the position that no change in traditional conceptualizations of jurisdiction is necessary when regulating the Internet is set forth in Jack L. Goldsmith, *Against Cyberanarchy*, 65 U. CHI. L. REV. 1199 (1998).

6. For the virtues of pragmatism in law discussed more broadly, see RICHARD POSNER, LAW, PRAGMATISM AND DEMOCRACY (2003).

7. *See infra* Part III.

8. *See, e.g.*, David G. Post, *Against "Against Cyberanarchy,"* 17 BERKELEY TECH L.J. 1365, 1381–86 (2002).

of government in enforcing law—as well as consider whether traditional deterrence is truly possible—so as to better protect privacy and industry.

A good example of the need for a better, but still pragmatic, approach to Internet regulation—and the example used throughout this article—is the federal CAN-SPAM Act (Controlling the Assault of Non-Solicited Pornography and Marketing Act), which took effect January 1, 2004.[9] The Act is in many ways exemplary legislation. The Act benefited from Congress's long debate over whether to restrict commercial email,[10] and is solicitous of the concerns of email recipients, non-commercial private senders, and legitimate businesses engaged in commercial email contact.[11] The CAN-SPAM Act imports concerns from both consumer advocacy groups as well as pro-marketing industry positions (notably, the Act's strong federal preemption position).[12] The law makes full use of the laboratory of the states, and contains provisions drawn from the preexisting state laws governing unsolicited commercial email, while discarding and preempting the most destructive state laws that threatened to govern all Internet traffic.[13] In many senses, therefore, the bill is the best Congress has to offer.

The Act is, nevertheless, flawed. The flaws result not from a lack of deliberation or considered drafting, but arise instead from fundamental and

---

9. CAN-SPAM Act, Pub L. No. 108-187, 117 Stat. 2699 (later codified at 15 U.S.C. § 7701) [hereinafter CAN-SPAM].

10. The Act was first introduced in 2000, and was substantially honed in the subsequent three years.

11. Prior versions of the CAN-SPAM Act were introduced in the 106th and 107th Congresses. H.R. 2162, 106th Cong. (1999); H.R. 1017, 107th Cong. (2001)).

12. *See* CAN-SPAM § 2(a)(11). Broad-reaching federal preemption was seen as a means to protect industry from varying state laws:

> Many States have enacted legislation intended to regulate or reduce unsolicited commercial electronic mail, but these statutes impose different standards and requirements. As a result, they do not appear to have been successful in addressing the problems associated with unsolicited commercial electronic mail, in part because, since an electronic mail address does not specify a geographic location, it can be extremely difficult for law-abiding businesses to know with which of these disparate statutes they are required to comply.

Id.

13. See CAL. BUS. & PROF. CODE, div. 7, pt. 3, ch. 1, art. 1.8, § 17529 (West 2003), enacted immediately prior to Governor Gray Davis's departure from office. The statute imposed draconian penalties, including statutory damages, for each instance in which an email was sent to or from a California computer without express prior consent by the recipient to receive the email. Given the amount of email traffic that passes through California's computer system and the impossibility of determining whether an email user was accessing his email address from the State of California, this statute was a major impetus behind the federal preemption provisions in the CAN-SPAM Act.

mistaken assumptions about the role of enforcement, deterrence, and government collectivization in Internet regulation. The flaws in the Act appear most clearly in four provisions.[14] First, the Act requires the Federal Trade Commission ("FTC") to consider and report on the creation of a do-not-email registry that would gather the email addresses of private users who do not wish to receive commercial email into a centralized database protected by the threat of government enforcement.[15] Second, the Act imposes criminal and civil penalties for fraudulent or misleading behavior (for example, misleading header information on an email) that are largely redundant of existing state and federal penalties.[16] Third, the Act preempts state laws that purport to govern unsolicited commercial email (but, importantly, does not preempt the application of general fraud and consumer protection statutes that incidentally impact the area of email communication).[17] And fourth, the Act effectively prohibits the commercial use of data architecture tools—such as webcrawling software[18]—that form the backbone of the Internet.[19]

The Act thus proposes to centralize personal information under dubious government protection, relies on proscriptions that have extremely limited enforceability instead of creating incentives to block the effects of out-of-jurisdiction acts, and prohibits the use of invaluable data architecture and Internet search tools for purposes of commercial (and quasi-commercial) contact.[20] As a result, the CAN-SPAM Act creates significant dangers for both the industry and the privacy interests it was meant to protect.

Section II of the article therefore frames the debate by asking whether Internet regulations can and should be seen as dealing with a common set of problems, or whether "cyberlaw" does not exist as a useful unifying concept. The section also addresses the academic literature to date as it discusses the problem of applying traditional notions of jurisdiction and enforcement to frequent and cheap cross-border transactions. The section concludes that unified standards for cyberlaws do exist, and sets forth the common set of Internet characteristics—e.g., collective action, cross-border

14. These provisions are in the order of discussion, not their order of appearance in the statute.

15. *See* CAN-SPAM Act § 9.

16. *Id.* §§ 4–6.

17. *Id.* § 8.

18. Webcrawling software is software that automatically seeks out and organizes information on the Internet. Spammers use webcrawling software to scan websites and usenet groups for email addresses, which they then spam. However, webcrawling software is also an integral component of Internet architecture tools such as the Google search engine.

19. *See* CAN-SPAM Act § 5.

20. *See id.* §§ 4, 5(b), 9.

enforcement, frequency and facility of transactions, and decentralization—that such laws must address in order to be successful.

Section III discusses the first foundational flaw of the CAN-SPAM Act: the Act ignores the potential for collective action focused *against* government-protected information. By collecting the email addresses of private users who do not want to receive unsolicited commercial email in a centralized, government-protected list, the Act drastically increases the risk that list participants will receive dangerous (i.e., viral or fraudulent) spam.

Section IV discusses the CAN-SPAM Act's reliance on traditional notions of enforcement and deterrence to control costless cross-border transactions. The section considers the possibility that the Act's harsh penalties, meant for criminal or intentional spammers, will be enforced almost entirely against legitimate companies and unwitting everyday Internet users. The section concludes that the obstacles to enforcement, and hence deterrence, of the Act are such that the Act's criminal and civil penalties provide little benefit, and may cause significant harm, to industry and privacy.

Section V shifts the debate from questions of jurisdiction and enforcement, and focuses instead on whether Congress should adopt new substantive rules to regulate specific technological characteristics. For example, the CAN-SPAM Act prohibits businesses from using webcrawling software to gather information about potential customers.[21] This restriction will have strong negative consequences for business, since webcrawling software is one of the primary and most useful types of computer tools for legitimate businesses. Common and innocuous business activities, from using Google to cutting and pasting from websites, fall under the wording of the statute and may be prohibited.[22]

Finally, Section VI makes several proposals for a positive pragmatic approach to Internet legislation. First, the section argues that the law should provide safe harbors for legitimate businesses to identify the unsolicited messages that they send. This approach would separate routine unsolicited commercial messages from viral or fraudulent messages, would lessen the risk that legitimate businesses would disproportionately suffer enforcement, and would permit enforcement resources to be focused on dangerous, rather than merely annoying, spam. Second, the law should provide strong incentives to adopt technological solutions that plug the holes in the Internet architecture that permit spam.

---

21. *See id.* §§ 2(a)(10), 5(b)(1)–(2).
22. *See id.* § 5.

Overall, this article concludes that a successful pragmatic approach to Internet legislation would include recognizing the practical weaknesses in government collectivization, enforcement, and deterrence as applied to transactions that have nearly no cost and nearly infinite frequency.[23] This article seeks to demonstrate that privacy and industry would be better served by laws that: (1) recognize the limitations of government as a form of collective action, as well as the obstacles to enforcement and deterrence in the Internet context; but (2) embrace an active role for law and government in promoting information exchange and facilitating individual efforts to protect privacy.

II. WHY THE DEBATE OVER THE NOVELTY OF THE INTERNET DOES NOT ADEQUATELY EXPLAIN OR PREDICT LEGISLATION

A. By What Standards Should Internet Regulations Be Measured?

Before a statute can be evaluated, the benchmarks against which it is to be measured should be set. Does it make sense to discuss regulation of the Internet as if it is a distinct category of regulation with a distinct set of problems and a common set of solutions as cyberlaw? Relatedly, does it make sense to criticize Internet regulations such as the CAN-SPAM Act for failing to foresee those common problems?[24] It has been argued that there is

---

23. The idea that traditional approaches to the role of government, enforcement, and deterrence will function without increasing risks to Internet privacy or commerce is termed "jurisdictional unexceptionalism." *See infra* notes 53–54 and accompanying text. Jurisdictional unexceptionalism has had the best success in academia as well as the legislature, thus I primarily address its failings. Note, however, that if an unrestrained exceptionalism were seriously proposed (for example, an argument that all new situations require new laws), it would create the same problems.

24. There is, of course, one body of law against which the shortcomings of all legislation are measured: the U.S. Constitution. Unsurprisingly, most of the criticism of Internet legislation to date has been that the laws are constitutionally improper. This criticism is probably due to the limitations on court challenges to legislation, rather than to any particular susceptibility on the part of legislatures considering Internet regulation to violate the Constitution. I do not level a constitutional argument here. Indeed, I find it unlikely that the regulation of the Internet is any more fraught with constitutional concerns than the regulation of any other aspect of human existence. Perhaps the newness of the medium caused legislators to initially miss their stride, resulting in the infamous Communications Decency Act. Communications Decency Act of 1996, Pub. L. No. 104-104, 110 Stat. 133 (codified at 47 U.S.C. §§ 223, 230, 560, 561 (2000)). However, both legislators and judges have grown more accustomed to the medium, leading to fewer egregious mistakes (on the part of legislators) and more acceptance of legislative judgment (on the part of judges). Thus, for example, even the most controversial provisions of the Children's Internet Protection Act, Pub. L. No. 106-554, div. B., tit. XVII, 114 Stat. 2763A-

no such thing as cyberlaw.[25] The death of cyberspace was announced in the late 1990s; by the year 2000, the Internet was supposedly viewed as a communications medium like any other, rather than an autonomous space in the process of developing its own norms.[26] According to this view, the fact that regular statutes now regulate various aspects of Internet activity forecloses any speculation that the Internet is a borderless medium that is in the process of developing its own set of rules.[27]

The fact that the Internet is now to a significant degree regulated by statute by no means indicates that there is no "law of the Internet," any more than the heavy regulation of the media indicates that there is no such thing as "telecommunications law."[28] Quite the opposite. Rules for regulation of the Internet have developed according to the same process as the common law elsewhere: business norms have developed into industry standards, which in turn are adopted by courts, and the resulting common law rules are codified by statutes. It would be quite surprising if the Internet had not been integrated into common and statutory law in the decade that it has captured the legal imagination.

No more should be expected of a category of law than that the category frame a set of problems and solutions. The term "cyberlaw" certainly does this. Indeed, if one were to approach other categories of law with the ontological parsimony shown by cyberlaw naysayers, no category of law could exist.[29] How is "torts" unified in any way that "cyberlaw" is not?

It might be easy to argue that "cyberlaw" in the sense of "British law" does not exist—hence the rejection of the place metaphor by some scholars—while "cyberlaw" in the sense of "telecommunications law" does exist. But that is too facile: there does exist a set of common problems and solutions that have been developed across jurisdictions unique to regulation of Internet behavior. These are not a unified set of laws, but rather responses to the same set of problems. Thus, there is a "cyberlaw"—that is, a set of responses by national and local governments, as well as industry customs and individual actions, that set up a framework for regulating

---

335 (2000), which required libraries to install "censorware" on public computer stations, were recently upheld by the Supreme Court by a solid majority. United States v. Am. Library Ass'n, 539 U.S. 194, 214 (2003).

25. *See* Joseph H. Sommer, *Against Cyberlaw*, 15 BERKELEY TECH. L.J. 1145 (2000); Wu, *supra* note 2.

26. *See* Wu, *supra* note 2.

27. *See id.*

28. It may be that in time the first will be subsumed into the second. For the time being, however, no other medium shares the cocktail of frequency, facility, and decentralization of cross-border transactions unique to Internet transactions.

29. *But see* Sommer, *supra* note 25.

Internet behavior. Some of these find their way into court opinions, others find their way into statutes, and still others remain merely "intuitions" or behavior norms by net users.[30]

Having defined cyberlaw also further defines the goal of this paper: to identify specific common problems to Internet regulation, and then evaluate a specific statute—the CAN-SPAM Act—based on its responses to those problems. There are four characteristics of Internet communication that have consistently presented interesting questions for Internet regulators. The first characteristic is the cross-border nature of the medium.[31] The second is the low expense of engaging in transactions.[32] The third is the ease of engaging in multiple contacts or transactions.[33] The fourth is the decentralized nature of the Internet architecture.[34] Although none of these characteristics itself is unique, the possibility of nearly infinite access to people in other jurisdictions, combined with the ease and low expense of such contacts, has operated to raise the frequency of cross-border transactions to an unprecedented degree.

These features of the Internet in turn have legal ramifications. The first is that the traditional role of government in organizing collective action may need to be reevaluated: The Internet facilitates collective action by citizens such that the government may not need to serve as an intermediary, and facilitates collective action by wrongdoers such that government involvement may simply provide a focal point for harmful behavior.[35] Second, enforcement is more difficult over the Internet, due to both the cross-border nature of the transactions, and the number of transactions involved.[36] Third, because enforcement is difficult, deterrence goals are

30. For an account of how cyberspace norms, often expressed as code, interact with legal norms, see generally LAWRENCE LESSIG, CODE: AND OTHER LAWS OF CYBERSPACE (1999).

31. *See* Goldsmith, *supra* note 5, at 1203.

32. Post, *supra* note 8, at 1374–76.

33. *Id.*

34. David G. Post & David R. Johnson, *And How Shall the Net Be Governed?: A Meditation on the Relative Virtues of Decentralized, Emergent Law*, *in* COORDINATING THE INTERNET (Brian Kahin and James H. Keller eds., 1997). As an aside, the issue of infinite duplication that plagues intellectual property law is a side effect of decentralization. The fact that a piece of intellectual property can be duplicated, even duplicated fairly cheaply, is not new. That revolution occurred with the printing press. However, the ability to distribute that information in identical form through a decentralized network, and for each recipient to share the entire benefit of the duplication at zero cost is the feature of the Internet that creates intellectual property problems. Thus, for example, the focus of the Recording Industry Association of America ("RIAA") in its attempt to stop music piracy has been to focus on the peer-to-peer distribution networks (the ultimate example of decentralization) rather than to limit the ability to duplicate the music.

35. *See infra* Part III.

36. *See infra* Part IV.

harder to meet.[37] And finally, there is a very real danger that ignoring these ramifications will cause legislators to create laws that strain too hard to reach out-of-jurisdiction wrongdoers, but instead only ensnare private users and legitimate businesses.[38] These four points provide a framework that I will use to evaluate the Act, and provide suggestions as to how Internet regulations can avoid these problems in the future.

B. The Debate to Date over Internet Regulation Has Centered Around Whether the Internet Constitutes a Sufficiently Novel Medium To Require Legal Innovation

The first academic discussions about the feasibility of Internet regulation focused almost entirely on the jurisdictional question.[39] The initial argument advanced was that cyberspace was an extranational medium that ought to be governed by a new law-set tailored to the medium akin to international trade law, treaty, or—such as it is—the law of outer space.[40] The response was that despite the innovations in technology, the behavior of real persons in realspace can be regulated without special resort to new law.[41] The oft-used line is that the Internet is a means of communication like any other, and that the actions of humans toward each other can be regulated whether by telephone, telegraph, or smoke signal.[42]

David Post recently described the two sides of the debate as "exceptionalist" and "unexceptionalist"—the principle being that unexceptionalists believe that little or no modification to the laws is required to govern wrongs conducted via a new medium, while exceptionalists argue that the novel characteristics of a medium merit new approaches.[43] This division drives Post's argument that changes in

---

37. *See* Post & Johnson, *supra* note 34.

38. *Id.*

39. Wu, *supra* note 2, at 171–73. Of course, questions of jurisdiction, enforcement, and deterrence are not completely divorced from the decentralized nature of the Internet. Centralization directly promotes government control of Internet activities, and correspondingly is directly linked to its ability to enforce and deter Internet behavior. Thus, countries that maintain a tight rein on their citizens' access to the Internet often do so by attacking the distributed nature of the Internet, and attempting to route Internet access through government-controlled entities. Goldsmith, *supra* note 5, at 1222–23.

40. David R. Johnson & David Post, *Law and Borders—The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367, 1370–76 (1996).

41. *See generally* Goldsmith, *supra* note 5.

42. *Id.* at 1201.

43. Post, *supra* note 8, at 1366–68 ("To the Unexceptionalist, whether a transaction occurs in cyberspace or realspace does not matter. . . . Those who think otherwise—Goldsmith calls

technology require changes in the law governing transactions that take place using that technology—even if only the frequency or facility of committing the wrong is altered.[44] Thus, for example, hacking laws were not necessary until computers became prevalent.[45] Of course, "unexceptionalists" would respond that law is not merely reactive, and that there are significant costs to creating law tailored to a new scenario if existing principles of jurisprudence will serve.[46] If I commit murder with a heretofore unknown means, or in a new and innovative manner, I can be prosecuted. Legislatures do not have to react and pass laws for each new means by which a wrong is committed.[47]

But there remains a fundamental philosophical disconnect between the literature and the laws as enacted. It is odd that unexceptionalists should term their interlocutors "regulation skeptics," while they themselves have become the intellectual progenitors of the current wave of new laws regulating Internet action.[48] Unexceptionalism and statutory innovation are largely philosophically exclusive. The substantive wrongs that Internet regulation proponents seek to prevent by means of new law are, largely, already regulated.[49] A consistent unexceptionalist would be the real regulation skeptic because there would be no need for new laws at all.[50] If unexceptionalists are right, after all, prior doctrine will cover the field pretty well, since nothing is new under the sun when it comes to humans harming each other.[51] Thus, under the unexceptionalists' own arguments, there would be no need to pass new laws balancing privacy and freedom of speech on the Internet, because our existing jurisprudence would be able to cope with the admittedly complex problems created by real people in realspace. In an unexceptionalist world, these existing laws would simply be extended to govern the new cases.[52] The problem, of course, is the failure

---

them 'regulation skeptics,' though I prefer the less loaded and more symmetrical term "Exceptionalists"—believe that cyberspace is somehow different . . . .").

44. *Id.* at 1372–73.

45. *Id.*

46. *See* Frank H. Easterbrook, *Cyberspace and the Law of the Horse*, 1996 U. CHI. LEGAL F. 207, 207–08 (1996); Sommer, *supra* note 25, at 1147–49.

47. *See generally* Goldsmith, *supra* note 5, at 1211–12.

48. *Id.* at 1202.

49. Thus, for example, fraud, defamation, or (as discussed by Goldsmith) copyright violations are already prohibited. *See id.*

50. *See* Suzanna Sherry, *Haste Makes Waste: Congress and the Common Law in Cyberspace*, 55 VAND. L. REV. 309, 310–11 (2002) ("Speed is an asset in computer technology, but not necessarily in law. The new technologies of the twentieth and twenty-first centuries have inevitably raised new legal questions . . . . But many of these perceived 'crises' could actually have been resolved by previously established law.").

51. *See id.* at 310–14.

52. *See id.* at 311–12.

to distinguish between jurisdictional exceptionalism and content exceptionalism, as described below.

C. *Jurisdictional Unexceptionalism and Hybrid Laws*

I use the term "jurisdictional unexceptionalist" in order to clarify this important point: there is a critical difference between "jurisdictional unexceptionalism"—the idea that traditional government proscription and enforcement will function to deter in the Internet context[53]—and "content unexceptionalism," which might draw on traditional rules governing a specific form of conduct in another context and apply it to the Internet. When a rule has been developed and successfully applied for other media—for example, rules governing unsolicited junk "snail" mail—that rule can and possibly should be applied to the same form of conduct (unsolicited commercial contact) over the Internet.[54] Thus, I use the term "jurisdictional unexceptionalist" to describe laws that are symptomatic of the belief that Internet behavior can and should be regulated by regular government-centered proscription, enforcement, and deterrence.

Once this distinction is made, the process of evaluating Internet regulations can begin. The laws that have been passed have been mixed. The program to "governmentalize"—or, indeed, federalize—the Internet has both exceptionalist and unexceptionalist portions: Congress is not only sanguine about the deterrent effect of proscriptive law despite the fact that the prime targets of these proscriptions are undetectable, or overseas, or both (jurisdictional unexceptionalism), but also willing to impose new rules on a medium where the medium does not meaningfully differ from other prior media of communication (content exceptionalism).

Symptomatically, the CAN-SPAM Act evidences both an "unexceptionalist" intuition that the prior rules of jurisdiction and enforcement will work as applied to the Internet, and an "exceptionalist" desire to regulate the Internet in new fashion by using rules tied to specific technological features.[55] This article argues that these intuitions are exactly wrong. Better laws would be achieved by reversing these intuitions, and

---

53. These three concepts—governmentalism, enforcement, and deterrence—do not all have to do with jurisdiction in the purest sense, but the fact that Internet transactions are often cross-border is the most commonly discussed obstacle to enforcement and deterrence, and thus used to justify government regulation of an area. Two equally important characteristics are, of course, the facility and frequency of the communications. *See* Goldsmith, *supra* note 5, at 1237–39.

54. *See infra* Part V.

55. For example, the Act prohibits the use of Internet architecture software (webcrawlers) to gather information about prospective customers. CAN-SPAM Act §§ 5–6.

enacting laws that are exceptionalist as a matter of jurisdiction—i.e., only contain limited proscriptions of behavior for extrajurisdictional parties, and do not rely on the deterrent effect of criminal provisions to function—but content unexceptionalist, in that they adopt tried rules already developed in the courts for balancing privacy interests against unsolicited commercial contacts.

III. THE CAN-SPAM ACT: PRIVACY AND INDUSTRY PROTECTION FOUNDED ON (FLAWED) JURISDICTIONAL UNEXCEPTIONALISM

Jurisdictional unexceptionalists must not only demonstrate that government laws can be enforced and will deter behavior in Internet transactions, they must also demonstrate that it is necessary for a government to take action in the first place. The standard justification for routing the collective resources of a community through a centralized government is that each individual would, alone, be unable to solve the problem.[56] Countries band together to build roads or armies. However, one of the critical differences between the Internet and other communications media is that the Internet uses a distributed architecture—tools are available at the level of individual users that are not available to people in "realspace."[57] Thus, the first question is whether the nature of the Internet or the transactions taking place over it merit re-examining the role of government in collecting resources and protecting commonly held resources.[58]

This section seeks to demonstrate that the distributed nature of the Internet alters—but does not eliminate—the role of government in orchestrating collective action. Failure to recognize the realities of collective action on the Internet may cause the forces of collective action to operate *against* the interests that the government is attempting to protect. When these considerations are ignored, even the most well-intentioned statute becomes a threat to personal privacy and industry.

---

56. For a description of the unique problems created by collective action in light of the decentralization of the Internet, see Amitai Aviram & Avishalom Tor, *Overcoming Impediments to Information Sharing*, 55 ALA. L. REV. 231 (2004).

57. The simplest example of this is the fact that while it is quite difficult for a regular mail recipient to screen all mail for junk mail, an email recipient can easily use filters to block most—but not all—unwanted contacts. How the law can improve the ability of private users to do so is a major focus.

58. From its inception, the Internet was a distributed architecture, placing tools at the local level, rather than in the hands of any specific controlling entity.

A. Centralizing Consumer Information Under Government Protection Threatens Personal Privacy

The privacy interests of individual users are made more vulnerable by any proposal to governmentalize consumer information in the form of a do-not-email database.[59] Do-not-contact lists have become the weapon of choice in recent years for restricting the ability of businesses to contact customers.[60] The CAN-SPAM Act followed this emerging trend,[61] and required the FTC to present a plan for setting up a nationwide "do-not-spam" list.[62] Such regimes are simple in principle. Instead of each

---

59. The FTC is instructed in section 9 of the CAN-SPAM Act to:

> (a) . . . [T]ransmit to the Senate Committee on Commerce, Science, and Transportation and the House of Representatives Committee on Energy and Commerce a report that—
>
> (1) sets forth a plan and timetable for establishing a nationwide marketing Do-Not-E-Mail registry;
>
> (2) includes an explanation of any practical, technical, security, privacy, enforceability, or other concerns that the Commission has regarding such a registry; and
>
> (3) includes an explanation of how the registry would be applied with respect to children with e-mail accounts.
>
> (b) AUTHORIZATION TO IMPLEMENT.—The Commission may establish and implement the plan, but not earlier than 9 months after the date of enactment of this Act.

CAN-SPAM Act § 9.

60. *See, e.g.*, the national do-not-call list, Telemarketing Sales Rule, 16 C.F.R. § 310 (2003).

61. *See* CAN-SPAM Act § 2(a)(1)–(4).

62. *Id.* § 9. Section 9 requires the FTC to:

> (1) set[] forth a plan and timetable for establishing a . . . nationwide marketing Do-Not-E-Mail registry; (2) [explain] any practical, technical, security, privacy, enforceability, or other concerns that the Commission has regarding such a registry; and (3) [explain] how the registry would be applied with respect to children with e-mail accounts.

Id. Pursuant to this requirement, the FTC submitted a sixty page report to Congress in June 2004. *See* FEDERAL TRADE COMMISSION, NATIONAL DO NOT EMAIL REGISTRY: A REPORT TO CONGRESS (June 2004), *available at* http://www.ftc.gov/reports/dneregistry/report.pdf [hereinafter "FEDERAL TRADE COMMISSION"]. At a June 15, 2004 press conference announcing the FTC's decision not to pursue creation of a do-not-spam list, FTC Chairman Timothy Muris explained that despite the success of the National Do-Not-Call list after which the CAN-SPAM Act modeled the do-not-email list proposal, such a registry was likely to lead to more harm than good in this case. He cited differences between email and phone numbers and security concerns related to an email list as the principle reasons for the Commission's conclusion. *See* Suzanne Choney, *FTC's Rejection of Anti-Spam List Is Facing Reality*, SAN DIEGO UNION TRIBUNE, June 21, 2004, *available at* http://www.signonsandiego.com/news/computing/choney/20040621-9999-mz1b21choney.html. The Commission's report concluded "a National Do Not Email Registry database would amount to the compilation of an extensive directory of active email addresses that currently does not exist," calling such a list of live email addresses a "gold mine" for spammers, and agreeing with many commentators who expressed the concern

individual user making use of self-help options (call blocking, email filtering) or business-by-business opt-out provisions, the government gathers the preference of everyone who does not want to be contacted in a central database. The government then imposes sanctions (usually either private or agency-enforced) for violation of the list.

In order for a list to be effective, businesses must be able to access the list in some fashion to determine who they may contact. The question is whether the accessibility of a do-not-contact list creates a greater problem of information privacy than would exist without a list. The answer is fairly straightforward. If the contact list is already generally known, then the creation of a do-not-contact list does not create an additional threat to privacy. Thus, for example, since telephone numbers are generally known or easily guessable,[63] the existence of a do-not-call list does not lower the privacy of telephone users. However, if the list of contactees is not generally known or easily guessable, then the creation of a list creates a threat to the privacy interests it is meant to protect.

There is no general list of email users, and individual email addresses are difficult to guess. Thus, the creation of a do-not-email list threatens the privacy interests it would purport to protect, if illegitimate spammers are willing to break the law and access the list to generate contacts, rather than restrict them. There are two ways for spammers to access the list: illegally, or legally. First, a spammer could hack the list by breaking whatever protection scheme is used to protect the list names. Gathering all list participants in one centralized database makes this easier, because the resources devoted to breaking centralized encryption are correspondingly greater. Second, a spammer could access the list as though it were a regular

---

"spammers would stop at nothing to obtain this list and misuse it to the detriment of consumers." FEDERAL TRADE COMMISSION, *supra*, at 24–25. "I wouldn't put my e-mail address on such a registry and I wouldn't advise consumers to either," Muris stated, explaining, "[c]onsumers will be spammed if we do a registry and spammed if we do not." *See* David McGuire, *FTC Says List Will Not Reduce Spam*, WASH. POST, *available at* http://www.washingtonpost.com/wp-dyn/articles/A43459-2004Jun15.html (June 15, 2004).

The threat of a do-not-email list remains a significant concern, despite the FTC's stance. Congressional supporters of the proposal have promised to continue to seek the implementation of such a list. New York Senator Charles Schumer, the main proponent of a do-not-spam list, issued a written statement expressing his disappointment with the FTC's decision, and promised to "pursue congressional alternatives in light of the FTC's adamancy." *See* Mark Harrington, *Fears of Making It Worse FTC: Do-Not-Spam Registry a No-Go*, NEWSDAY, June 16, 2004, at A5, *available at* 2004 WL 81479932. In addition, public support for a do-not-spam list remains strong, and several grassroots organizations continue to push for it. *See* Choney, *supra.*

63. Even unlisted numbers exist within regular calling blocks, thus, guessing a telephone number is not difficult.

legitimate business, but use the information instead to contact list participants.

B. Security Monoculture: Why Governmentalizing Personal Information Creates Security Risks

Governmentalizing the protection of personal information creates an information security monoculture, and increases the risk that a list will be hacked. The concept of a "security monoculture" is that as the amount and value of the information protected by any given security scheme increases, so too grow the incentives to break the scheme, as well as the resources devoted to breaking the scheme.[64] For example, regardless of the sophistication of the protections included in the Microsoft operating system, that system will *always* be more vulnerable to hacking than any other system—because the incentives for breaking the protection are much greater.[65]

The problem of security monoculture threatens any user who discloses his name to a do-not-email list: a centralized list is more likely to be hacked, and the list-participant spammed, than if the list-participant simply did not disclose the information at all. There is no reason to believe that the government will provide better protection than is already commercially available.[66] And high-grade commercial safeguards protecting email lists are hacked on a regular basis in the commercial sector.[67] For example, in October of 2003, Orbitz, a travel agency with an extensive email customer list, was hacked and the list of customers (the author included) was spammed.[68] One Internet commentator discussing the Orbitz hack put the

64. The term, although used generally in technology literature, is agricultural in origin, the idea being a crop or ecosystem that relies on a single element is more likely to be damaged. *See, e.g.*, Christopher D. Stone, *Beyond Rio: "Insuring" Against Global Warming*, 86 AM. J. INT'L L. 445, 486 (1992) (discussing risks of agricultural monoculture).

65. *See generally* Dan Geer et al., *Cyber*Insecurity: *The Cost of Monopoly*, Computer and Communication Industry Association White Paper, Sept. 23, 2003 (discussing information security problems created by the federal government's reliance on Microsoft's operating system) *available at* http://www.ccianet.org/papers/cyberinsecurity.pdf.

66. This is because the mathematics underlying all encryption is the same. *See infra* text accompanying notes 73–74.

67. *See, e.g.*, Alorie Gilbert, *Orbitz Investigates Security Breach*, CNET NEWS.COM, October 28, 2003, *at* http://news.com.com/2100-1038_3-5098644.html (noting that the company's email list had been hacked and spammed).

68. *See id.*

problem succinctly: "Now imagine if spammers were somehow able to grab the 'do-not-spam' registry . . . being proposed by several lawmakers?"[69]

The reason that government encryption will not outperform commercial encryption is that the fundamental mathematics underlying all encryption is essentially the same.[70] Encryption is a matter of making a "key" that a potential hacker has to guess in order to break the encryption.[71] The larger the key, the more time-consuming the key is to break—and to use. Keys can be made large enough to withstand most attempts to break them, but large keys will bog networks down, and are not useful for systems that must be very accessible.

Although vastly simplified, trying to crack a key can be analogized to trying to guess a telephone number. If the number is 3 digits long, it will not take long to guess all combinations. If the number is 500 digits long, it will take much longer to guess. Although the length of the number increases the difficulty of guessing the number, the mathematics of guessing the correct series of digits does not change. The critical determination for guessing the number is the amount of time and resources devoted to guessing. The same is true for encryption. Encryption can be broken; the question is how many CPU cycles can be devoted to breaking the encryption.[72] How many resources are devoted to breaking the encryption is determined by the

---

69. *See Orbitz Hacked by Spammers?*, BROADBANDREPORTS.COM, *at* http://www.broadbandreports.com/shownews/34962 (last visited Nov. 22, 2004).

70. For a general introduction to cryptography and its mechanisms, see NIELS FERGUSON & BRUCE SCHNEIER, PRACTICAL CRYPTOGRAPHY (John Wily & Sons 2003).

71. When discussing encryption of lists, two different techniques should be distinguished (I use the term "encryption" for both techniques in the main text). Pure encryption denotes a reversible process, whereby the information can be returned from its encrypted form to a non-encrypted state. "Hashing" denotes an irreversible process by which information is transformed such that it is impossible to be certain what the original information was. Hashing implies loss of information—the hash of an email address is a number from which it is impossible to compute the original, because a huge number of different originals—nearly all of which are unused email addresses—result in the same hash number. The value of hashing is that multiple "inputs" map to the same "output," such that one cannot guess which "input" or email address, is live based only on the "output" (the hashed number of the registered email address modified by the hashing algorithm). Hashing will dramatically reduce the problem of decryption, since it is impossible to perfectly decrypt a hashed list. However, such a list will always pose a non-zero risk of multiple legitimate inputs mapping to the same hashed output. This risk can be reduced, but not eliminated. And dictionary attacks, *see infra* note 75 and accompanying text, can raise the probability of reversing even hashed information, i.e., of guessing email addresses, as discussed *infra* note 77.

72. Even if parties are not attempting to hack the encryption, the more extensive the encryption, the more computer resources will be consumed in using the secure system. A do-not-email list will have to be highly accessible, and cannot become bogged down under many communications. This is yet another reason that military-level security will not be used to secure a consumer email list.

reward for doing so. The centralization of information in the hands of a government-protected list increases the incentives for breaking the encryption protecting a list of, for example, 50 million list participants, whereas the incentives for stealing a single consumer's private information are much lower, and probably not worth the effort.

There is a further question of incentives: will individuals take adequate precautions with personal information if they believe that information is government-protected? Individuals can take measures to preserve security that the government cannot. Even the simplest measures—such as maintaining an email address with a local ISP provider rather than with Yahoo or Hotmail; not placing the address on usenet groups or websites; and choosing a non-standard (i.e. non-name) email address—provide strong protection against spam. When combined with spam filters of even moderate sophistication—so that the rare spammer who does hit on the correct combination never learns of his success—and ISP-based spam-prevention measures, an individual has largely solved the spam problem, with no government involvement whatsoever.

A critic might point out two problems with this analysis, but both are ultimately unconvincing. The first potential criticism is that concentration of value draws concentration of effort to steal that value in realspace as well. Fort Knox might be considered a focal point for bank robbers, and the incentives to crack security might be correspondingly higher than to rob an individual taxpayer's house. Obviously, this realspace example demonstrates that when government security is vastly superior to individual precautions—at a not-disproportionately greater cost—collecting valuable items or information in the hands of the government is a successful defensive strategy. However, again, there is no reason to believe that government encryption is better than commercially available encryption, at least within the acceptable costs for running a highly accessible list. Moreover, there are geographical limitations on the collective ability of wrongdoers to successfully cooperate to perform a realspace wrong—again, for example, bank robbery. Though millions of people cannot collaborate to rob a realspace bank, it is fairly common practice for many different participants to crack encryption by contributing processing cycles from many individual computers.[73] Moreover, the fact that information can be costlessly and infinitely duplicated also alters the incentives to engage in

73. For a more benign version of this phenomenon, the Search for Extraterrestrial Intelligence (SETI) project offers a downloadable screensaver that borrows otherwise unused CPU cycles on personal computers to scrutinize data. *SETI at Home*, *at* http://setiathome.ssl.berkeley.edu/about_seti/about_seti_at_home_1.html (last visited Jan. 15, 2005).

collaborative action to steal centralized information. Unlike dividing the loot from a realspace bank robbery, where the number of participants reduces the benefit from the illegal action—while, presumably, the jail sentence deterring participation would remain the same—the spoils of a successful hack can be duplicated and each participant can benefit in full from the stolen information, thus raising the incentive of each hacker to contribute.

A second criticism of this analysis might be that more valuable secrets than email addresses—such as national defense secrets, or tax information—are already centralized in government hands. Surely, then, centralizing email addresses in government hands cannot pose any greater risk. Yet government protection—especially of military secrets—takes the above considerations into account: access is restricted, pinging (see discussion below) is not permitted, and larger encryption keys are used, despite the cost to users in terms of bandwidth and computer processing cycles. And the most secure secrets of all are simply not recorded on a network connected to the Internet.[74] A do-not-email list, however, must be generally accessible over the Internet to every legitimate business—including those with dial-up modems and outdated systems—that wish to scrub customer contact lists. Military-grade encryption of a consumer email database would simply bog the system down into unworkability.

On the other hand, individuals are not subject to the security monoculture problem. Individuals can actually make use of much weaker protection—and encryption keys that are less time-consuming and costly in terms of bandwidth and hardware to use—because the return for a given hacker in finding out any one person's private information is very low. This reduces the incentives to break any one encryption scheme, and thus reduces the resources devoted to decryption. In turn, laws that gather valuable information resources in government hands ought to consider the problem of reverse collective action, and the question of whether government involvement simply creates a focal point for wrongdoers.

C. The Ping Problem: Why a Do-Not-Email List That Followed the Do-Not-Call Model Would Threaten Privacy Even Without the Risk of a Hack

If a do-not-email list is to be used in the same fashion as the federal do-not-call list, the do-not-email list must be accessible to legitimate businesses

74. A private network unconnected to the Internet, or a computer otherwise unconnected to the Internet, can be termed a "cold vault." Cold vaults are routinely used to ensure data security from Internet attack.

that need to know who they may not contact. However, the necessary accessibility of the list creates the potential for any list to be used as a spammer research tool, rather than as a shield for list participants. A spammer might choose to use the database to identify who is on it in order to send them *more* spam, instead of less. Even if the list's protection is secure, for the spammer, a negative result is as good as a positive result—because an answer "no, you may not send email to a person on the list" identifies them as a live human being who can be spammed.

"Pinging," in this context, is the practice of asking the do-not-email list whether an email address generated by a random plausible guess—or "dictionary attack"[75]—is present on the list for the purpose of spamming it, rather than for the purpose of removing that address from an advertiser's customer contact list.[76] Even if the security schemes protecting the list remain intact, the responses from the list will tell the spammer what he or she needs to know: whether the address in question is a "live" address with a human on the other end. The result is that the existence of a pingable list improves the ability of spammers to identify and spam live addresses generated by a dictionary attack.[77]

The ping problem explains why the model of the national do-not-call list will not function in the email context. In the telephone context, a legitimate business contacts the list periodically and updates its internal records as to what numbers may be called. Of course, since all telephone numbers are known (or the cost of guessing is low), anonymity is insignificant

---

75. A dictionary attack is a computerized attempt to simply guess email addresses by combining words or letters in random combinations, permitting a spammer to send spam simply by guessing a plausible email address. The problem with dictionary attacks is that they are guesswork, and, after the passage of the CAN-SPAM Act, illegal. *See* CAN-SPAM Act § 4(a)(4). However, a dictionary attack combined with the ability to ping a central do-not-email server would vastly increase the ability of spammers to reduce guesswork by checking their dictionary attack against the list.

76. Generally, a "ping" is simply a message sent by one computer to another to tell if the second computer is connected to the network and listening for contacts. However, the term has been extended to mean practices whereby simply contacting another computer gives the sender of the ping the information required.

77. On an extremely technical note, hashing the list might seem to help with the ping problem but it probably does not. *See supra* note 71. While a wide range of purely randomly generated email addresses could hash to the same "No, do not email," (so the spammer would not know which of the strings was the "good" address), dictionary attacks are not purely random. Rather, a dictionary attack tries to guess commonly used plausible strings. For example, the guess that an email address ends in "@aol.com" will be much more profitable than a guess that the email address ends in "@sGS.XcW." To put it another way, a dictionary attack is likely to guess only strings that look like an email address and not guess random strings that look like gibberish. The hash will add little security, therefore, because the probability that another plausible string maps to the same output as a real address is small. For this reason hashing may not, in practice, be strong protection against pinging.

protection. Thus, for a telephone user, participating in a list carries no downside cost. Email addresses are presumptively anonymous, however. There are no blocks of easily guessable email addresses—and email anonymity is arguably the best privacy protection currently available.

Because anonymity is valuable in the Internet context, businesses cannot be permitted to simply download a list of email addresses they are not supposed to contact.[78] In order for a list to have any possibility of retaining the anonymity of list participants, the centralized database would have to be encrypted even from legitimate businesses that wish to use the list to "scrub" their own lists. Instead of downloading the list for use in scrubbing customer contact lists, businesses would submit their lists of customer contacts to the centralized do-not-email database. That customer list would then be encrypted,[79] and the encrypted customer list compared to the encrypted do-not-email list. The list would then generate a response indicating whether or not the mailer could contact the party in question.

However, the encryption of the list does not protect the identity of the parties on the list. If a spammer were to determine that a given email address was on the list, he has gained valuable information: an email address that he previously guessed might lead to a human being now has been confirmed. But there is no way to avoid this problem. In order for the list to function, it must inform legitimate businesses that a listed email address is off limits.

When I have given this article as a talk, a question usually arises here. One form of the question is: "Why does the list have to give any 'no' answer at all?" Another version of the question is: "Why doesn't the list just respond 'yes, you may email,' and give no further response?" A third version of the same question is: "Why can't the list just respond 'no' to the set of addresses that the list cannot identify, thus destroying the ability of a spammer to use the list to differentiate between guesses and live addresses?" The answer is that these responses would destroy the usefulness

78. It would be possible for businesses to download the encrypted list and submit their queries to the list on their own system. This would save bandwidth. The difficulty with permitting businesses to download the encrypted list is that the agency maintaining the list loses the ability to control the speed and frequency of an attempt to ping the list. Imagine pinging as trying to guess someone's password. Many systems will only let you guess a limited number of times before stopping further access. The FTC couldn't limit "wrong answer" pinging because the list by definition will not know the difference between an email address that is not on the list and an email address that does not exist. But the FTC could limit the number of contacts overall, for example. A dictionary attacker will likely need to ping the list with hundreds of millions of guesses. A legitimate business could probably be limited to checking its customer service lists which may rarely top a few million. Thus, retaining control over the list is likely the best way to proceed if the FTC does not wish to permit unrestrained pinging.

79. More accurately, the list would be hashed. *See supra* note 71.

of the list. An "unknown" query must receive the response "yes, you may email" because the list does not know every email address of everyone in the country. The list has no way to tell whether the email address that has been submitted is randomly generated, or belongs to someone who is not on the list. Conversely, if a person chooses not to sign up for the list, their address will be unknown to the list, and should generate a "yes, you may email." Thus, if the list is to function, *only* live email addresses of list participants will receive the "no, do not email" response, thus making them additionally likely to receive spam. By pinging the list, and spamming the list of "no, do not email" responses, a spammer will vastly improve his guesswork, and thus his ability to target live human beings by way of dictionary attacks.

There are ways to improve the security of the database, and mitigate the ping problem, but these involve increased expense and routing all commercial email through government servers. The system could be constructed such that the list would not return any message at all back to the originator. Instead, the federal agency responsible for enforcement would become a mass re-mailer. Permitted mails would be forwarded, while impermissible ones would simply disappear. But resending is vastly more expensive than the simple listing function provided by the federal do-not-call list. Although routing all commercial email through government servers would ping-proof the system, it would also create a government-managed bottleneck for all commercial email traffic, and create other, massive, security risks.[80]

D. Centralizing User Information Creates Opportunities for Fraud

In addition, the existence of a do-not-email list affords opportunities for fraud to true spammers. Parties that mimic, or hack, the sign-in portions of a federal do-not-email list have a ready-made tool for convincing users to reveal their email addresses. Already a staple of the Internet fraud trade is sending email notifications that look like official notices, containing hyperlinks to expertly-forged sites where parties enter their personal information.[81]

---

80. The costs of such a bottleneck going down, or otherwise becoming infected with a virus, or similar events, would be colossal. With a hack of such government server farms, a hacker could infect all commercial email in the United States with their virus in a single hack.

81. This practice is called "Phishing." *See* FTC Alert, *How Not To Get Hooked by a 'Phishing' Scam*, *at* http://www.ftc.gov/bcp/conline/pubs/alerts/phishingalrt.htm (noting that "[p]hishing[, also called 'carding,'] is a high-tech scam that uses spam . . . to deceive

Indeed, in the months prior to the rollout of the do-not-call list, some telemarketers began calling users, telling them that they would register the users for the national list. A similar fraud is increasingly common on the Internet. In a site-forgery scam (called "phishing"), an email mimicking a bank notification is sent to Internet users, requiring the user to log in to his bank account and review some charge or change. The site that the hyperlink directs the user to is, of course, forged, and captures the user's information. The user is then usually given a message that all is well with the account, and instructed to log off, or occasionally directed to the actual banking site. By creating a site where tens of millions of users will be registering previously closely-held email addresses, and by encouraging users to reveal their email addresses over the Internet, the do-not-email list merely creates a golden opportunity for parties seeking to cheaply gather millions of email addresses.[82] For example, in early February of 2004, authorities discovered a fraudulent website that held itself out as a federal do-not-email site.[83] The website, www.unsub.us was, for several days, up as a near-mirror image to the federal do-not-call list.[84] The dangers created by the site were therefore exacerbated by the fact that the site creator was able to mimic a government sponsored site, and as a result successfully convince people to release their private information.[85]

E. Centralizing Private Email Addresses in a Government Database Increases the Risk of Government-Sponsored Spam and Threatens Other Privacy Interests

There is one additional risk to private users who disclose their email addresses to a government-held do-not-spam list. The government is currently a source of significant spam. Congress has exempted itself from do-not-contact lists in the past. For example, the federal do-not-call list does not bar political telemarketing calls.[86] Congress has also exempted itself from the CAN-SPAM Act's anti-contact provisions.[87] Indeed, at the same

---

[consumers] into disclosing [their] credit card numbers, bank account information, Social Security number[s], passwords, or other sensitive information").

82. *See* FTC Press Release, *Sham Site Is a Scam: There Is No "National Do Not E-mail Registry," at* http://www.ftc.gov/opa/2004/02/spamcam.htm (Feb. 12, 2002).

83. *See id.*

84. *Id.*

85. *See id.*

86. *See* Telephone Consumer Protection Act, 47 U.S.C. § 227(a)(3) (2000).

87. *See* Jennifer S. Lee, *We Hate Spam, Congress Says (Except Ours)*, N.Y. TIMES, Dec. 28, 2003. More accurately, the CAN-SPAM Act simply does not apply to political speech because it is not commercial.

time that Congress was considering the Act in late 2003, the House Administration Committee voted to allow email messages to subscribers to congressional constituency lists during the 90-day blackout period prior to an election.[88]

The ability to deliver political spam depends on the ability to match private email addresses to voter registration records. Currently, consumer information vendors compare voter registration records with registries of names and email addresses gathered from the net, and sell the resulting matches—representing email addresses of constituent voters—to members of Congress.[89] As of December 2003, some 40 House members reportedly bought or planned to buy such lists.[90] A proposed do-not-email list would give those addresses to government agencies for free.[91]

This matters because the law contains no restrictions on what the government might do with a private list of email addresses outside of its role as list keeper. To the extent that Internet addresses can be matched with profiles in order to connect a person with his Internet signifier, that connection can be used to monitor the sender's communications if an agency were to so desire.[92] At the very least, a user who reveals his Internet identity to a centralized government database has connected a real person to the ISP that provides the email account.[93] Because of these broader privacy concerns, at the very least the FTC should articulate privacy standards and use restrictions clearly setting forth how and under what circumstances the government would be permitted to make use of the list.[94]

---

88. *Id.*

89. *See id.*

90. *Id.*

91. This is not to say that no beneficial effects could come of exempting government from a bar on unsolicited contact. For example, in the instance of a massive virus attack, a critical virus fix could be distributed through the email system. Or, similar to weather warning systems, news of critical and immediate national importance could also be distributed via email. However, other channels exist for distributing at least some of this information (for example, websites), that do not present questions of expropriation of private information for government use.

92. *See* Will Thomas DeVries, *Protecting Privacy in the Digital Age*, 18 BERKELEY TECH. L.J. 283, 294–95 (2003); John Schwartz, *FBI's Internet Wiretaps Raise Privacy Concerns; New System Tracks Suspects Online*, WASH. POST, July 12, 2000, at A1 (discussing FBI use of email interception programs) *available at* 2000 WL 19618793.

93. *See* DeVries, *supra* note 92, at 294.

94. One very effective technique that would improve both privacy from hackers and from the government would be to require the FTC to only keep a hashed version of the list (*see supra* note 71) rather than keep the list as a normal database, albeit protected by encrypted access. As soon as a user submitted his or her name to the website, that address would be hashed, such that nobody could use it, but any business submitting that same email address to the list would be informed that he or she would not be permitted to contact it. Pinging would still be a problem, but a hashed list would serve quite as well as an encrypted list for purposes of keeping the

IV. REEVALUATING THE ROLE OF ENFORCEMENT AND DETERRENCE IN LIMITING INTERNET TRANSACTIONS

The next basic premise of jurisdictional unexceptionalism is that enforceability and deterrence are unaltered by the medium in which the actions to be deterred will take place.[95] Thus, the jurisdictional unexceptionalist will argue that the real actions of real people in realspace can be deterred because the laws can reach them. For example, although the jurisdictional questions of cross-border criminal prosecutions are complex, a jurisdictional unexceptionalist would indicate that such problems are no more complex by virtue of the fact that the acts were done via the Internet, or telephone, or facsimile.[96]

However, these technologies do not share either the frequency or facility of Internet communication.[97] Further, the jurisdictional problems created by the Internet *are* more complex than before, because Internet wrongdoers seek out lawless jurisdictions from which to launch their operations.[98] Thus, Internet regulations that do not take the significant obstacles to enforcement—and thus deterrence—into account damage the very private users and legitimate businesses they mean to protect.

A. The CAN-SPAM Act's Unenforceable and Redundant Criminal Provisions Do Not Add to Deterrence

The CAN-SPAM Act offers a set of criminal prohibitions that piggyback onto other state or federal substantive crimes.[99] The Act's penalty provisions first bar fraud and similar activity by use of electronic mail.[100]

---

government from misusing the information because it would only have the hashed (and effectively non-decryptable) version of the list.

95. Goldsmith, *supra* note 5, at 1250.

96. *Id.*

97. Post, *supra* note 8, at 1376.

98. *See infra* Parts IV.A.3–4. Although Goldsmith hypothesizes that, for example, the jurisdictional problems of resolving copyright questions are no more difficult for an analog book seller (AnalogBooks) than for an online book marketer (DigitalBooks), his hypothesis omits one element: it is easier for DigitalBooks to relocate to the Palestinian Territories (for example) and thus operate beyond the reach of the copyright holders. *See* Goldsmith, *supra* note 5, at 1204–05; Post, *supra* note 832, at 1366–73.

99. CAN-SPAM Act §§ 4–6.

100. Section 4 of the CAN-SPAM Act adds § 1037 to Chapter 47 of Title 18 of the United States Code, and states:

> § 1037. Fraud and related activity in connection with electronic mail.
>
> (a) IN GENERAL.—Whoever, in or affecting interstate or foreign commerce, knowingly—

Thus, the Act makes the practices of "spoofing" (altering header information to mislead the recipient as to the sender of the email) and "spacking" (hacking a computer in order to use that computer to send the spam, leaving a dead-end trail at an innocent user's computer) federal offenses.[101] The Act contains a separate set of provisions, requiring senders of unsolicited commercial emails to provide identifying information, a real-world address, and a means to opt out of further unsolicited communications.[102]

1. The Act Punishes Fraud With Respect to the Sender of a Commercial Email Message

The punishment for falsifying the identity or path of an email message depends on whether the action was completed in violation of other state or federal law.[103] For example, the term of imprisonment set by the Act is five

---

(1) accesses a protected computer without authorization, and intentionally initiates the transmission of multiple commercial electronic mail messages from or through such computer,

(2) uses a protected computer to relay or retransmit multiple commercial electronic mail messages, with the intent to deceive or mislead recipients, or any Internet access service, as to the origin of such messages,

(3) materially falsifies header information in multiple commercial electronic mail messages and intentionally initiates the transmission of such messages,

(4) registers, using information that materially falsifies the identity of the actual registrant, for five or more electronic mail accounts or online user accounts or two or more domain names, and intentionally initiates the transmission of multiple commercial electronic mail messages from any combination of such accounts or domain names, or

(5) falsely represents oneself to be the registrant or the legitimate successor in interest to the registrant of 5 or more Internet Protocol addresses, and intentionally initiates the transmission of multiple commercial electronic mail messages from such addresses,

or conspires to do so, shall be punished as provided in subsection (b).

18 U.S.C. § 1037(a) (2000).

101. CAN-SPAM Act, § 4.

102. CAN-SPAM Act, § 5(a)(5).

103. *Id.* § 4(b) indicates:

Penalties.—The punishment for an offense under subsection (a) is—

(1) a fine under this title, imprisonment for not more than 5 years, or both, if—

(A) the offense is committed in furtherance of any felony under the laws of the United States or of any State; or

(B) the defendant has previously been convicted under this section or section 1030, or under the law of any State for conduct

years if the misleading email header information was used in the commission of a felony under federal or state law, or if the defendant was previously convicted under any law prohibiting transmission of multiple commercial electronic mail messages.[104] The same conduct is subject to a three-year sentence if the user either hacks a computer (subsection (a)(1)), or falsifies information in order to obtain twenty or more email accounts, or ten domain names.[105] Similarly, the use of false or misleading header information may be punished with a fine, a three-year sentence, or both, if more than 2500 messages were sent during any 24-hour period, 25,000 during any 30-day period, or 250,000 during any one-year period, or if the offense caused an aggregate loss of $5000 to any person or persons within a one-year period.[106] Finally, the Act imposes a three-year sentence for committing any of the proscribed actions in concert with three or more other people, if the defendant occupied a leadership role.[107] All other instances are punished with a fine, or up to one year in prison.[108] In addition, the Act provides for the forfeiture of illegal gains or computer equipment used to facilitate the offense.[109]

2. Federal Criminal Spam Laws Offer Limited Additional Deterrence

However, the deterrent effect of the statute is minimal because the criminal provisions are, by design, redundant of state and federal laws that impose harsh penalties. Spackers—and most of the worst spammers—are already in violation of state and federal law. For example, prior to the passage of the CAN-SPAM Act—and its subsequent preemption of most state laws governing unsolicited commercial email—Virginia adopted a tough anti-spoofing law making the practice a felony.[110]

Similarly, hacking is already a federal crime.[111] When a spam-hacker makes use of another person's computer as a "dead end" source for spam, he is already risking criminal conviction.[112] For this reason, FTC chairman

---

involving the transmission of multiple commercial electronic mail messages or unauthorized access to a computer system.

104. *Id.*
105. *Id.* § 4(a)(4), (b)(2)(B).
106. *Id.* § 4(b)(2)(C)–(D).
107. *Id.* § 4(b)(2)(F).
108. *Id.* § 4(b)(3).
109. *Id.* § 4(c).
110. VA. CODE ANN. § 18.2-152.3:1 (Michie 2003).
111. *See, e.g.*, 18 U.S.C. § 1030 (2000).
112. *Id.*

Timothy Muris—a supporter of the federal do-not-call list—has repeatedly and publicly stated that most spam already violates both federal and state law and that adding more criminal provisions without addressing the enforcement problem will not make a significant difference.[113] Muris noted that the problem with enforcement of an anti-email list is both the decentralized nature of the Internet, and the facility of cross-border communications: "The beauty of the Internet, of course, is that you can E-mail anybody, anywhere in the world. The bane of the Internet is that anybody, anywhere in the world, can E-mail you."[114] Muris noted that enforcement against overseas spammers would be nonexistent because of the routine use of aliases or the use of hacked computers and routers for spam.[115]

3. The CAN-SPAM Act's Criminal Provisions Are Largely Unenforceable Against Out-of-Country Spammers

The CAN-SPAM Act's provisions are not enforceable against the parties they are intended to deter: the problem remains the volume and traceability of communications, as well as the susceptibility to identification, arrest, and extradition of the parties engaged in the proscribed activity. Thus, extranationalism again appears as a factor despite the reassurances of unexceptionalists that cross-border bad actors can be caught and punished.[116] The worst spammers operate from outside the country, and increasingly choose to do so from places where the reach of even international law is attenuated or nonexistent.[117] For example, a Polish consortium continues to offer to immunize spammers from *traceroute* and other Internet tracking programs for a $1500-a-month fee through a double-blind routing service by using spacked computers.[118] Outside of the spam context, the Napster-clone Earth Station Five operates from the Jenin refugee camp, and, at least to date, has successfully resisted the increasingly concerned enforcement attempts of the MPAA and RIAA.[119]

---

113. Jennifer C. Kerr, *FTC Chairman Doubtful That Anti-Spam List Will Help*, INFO. WK., Mar. 11, 2004, *available at* http://www.informationweek.com/shared/printableArticleSrc.jhtml?articleID=18312071.

114. *Id.*

115. *Id.*

116. Goldsmith, *supra* note 5, at 1203–04, 1216–21.

117. Kerr, *supra* note 113.

118. *See* Brian McWilliams, *Cloaking Device Made for Spammers*, *at* http://www.wired.com/news/business/0,1367,60747,00.html (Oct. 9, 2003).

119. *See Sex, Lies and Earth Station 5*, ECONOMIST, Dec. 18, 2003, *available at* http://www.economist.com/printedition/displayStory.cfm?Story_ID=2301336.

4. Enforcement Is Limited Against Even In-Jurisdiction Spammers

Even those spammers—especially pornographers—who are inside the country are unlikely to be effectively deterred. In a practice known as "spacking," spammers commonly use hacked personal computers as dead-end drop-boxes for their stock-in-trade. Spacking is the function of an alliance between spammers and hackers. Computers using the Windows operating system, usually owned by private and innocent Internet users, are used to host the pornography site or send the spam email without the owner's knowledge. The goal of the spacker is to leave a cold trail, ending at an innocent user's front door. Examples of spam-hacking include fronting a pornography website on a linked ring of hacked personal computers, or forwarding spam email that, when traced, only leads back to the hacked personal computer. Hacked computers are also used as secure sites from which to launch further hacking attacks. Thus, even if an enforcing agency were to trace the most virulent forms of spam—such as pornography, fraudulent emails, and virus-laden emails—the path would dead end at an innocent party's private computer. Thus, not only is enforcement of criminal penalties against sophisticated spammers unlikely to be effective, but the very structure of how such spam is sent means that law enforcement agencies will inevitably attempt enforcement against innocent parties.

B. The Act's Civil Penalties Do Not Add to Deterrence

The Act contains a second set of prohibitions and requirements, which are backed by civil penalties and statutory damages. Section 5 of the Act sets out a series of requirements that senders of unsolicited commercial email must meet or face liability. The section prohibits false transmission information[120] and deceptive subject headings.[121] Section 5 also requires senders to include a return email address that the recipient may use to object to further contacts,[122] and prohibits further contacts once a recipient has opted out of future messages.[123] Finally, the section requires a sender to include its physical (realspace) address, a conspicuous identifier that the email is an advertisement, and a clear and conspicuous notice of the opportunity to opt out of receipt of future messages.[124]

120. CAN-SPAM Act § 5(a)(1)(A)–(C).
121. *Id.* § 5(a)(2).
122. *Id.* § 5(a)(3)(A)(i)–(ii).
123. *Id.* § 5(a)(4).
124. *Id.* § 5(a)(5)(i)–(iii).

One important new concept set forth in the Act is that businesses will be held liable for knowingly permitting their products to be marketed by means of violations of the Act.[125] This fills an important gap in prior laws, which had promoted a "don't ask" mentality by businesses that hired advertising firms to handle their online promotional activity. Section 6 of the Act targets businesses that knowingly promote their products by means of electronic mail.[126] Thus, violations of Section 5 of the Act can be attributed to the person who benefits from the promotion if the person should have known that his product was being promoted in electronic messages, expected to receive an economic benefit from the promotion, and took no action to prevent the transmission of the message.[127]

The civil prohibitions of the Act are enforced by the FTC under its enforcement powers to bar unfair trade practices,[128] and by state attorneys general, who may bring actions to recover the actual damages caused by the infraction, or statutory damages of $250 per email, whichever is greater.[129] The Act contains no private right of action, but does permit an ISP to bring a civil action in federal court.[130] State attorneys general and ISPs may use these actions to recover either actual or statutory damages on a per-infraction basis.[131]

However, these civil penalties will not deter spammers either. Prior to the passage of the Act, most of the states had enacted individual anti-spam provisions, which permitted individual rights of action, and enabled state

---

125. *Id.* § 6(a).

126. *Id.*

127. *Id.* § 6(a)(3)(A)–(B).

128. *Id.* § 7(a); 15 U.S.C. § 57a (2000).

129. The per-infraction measure of damages is limited to $2,000,000. CAN-SPAM Act § 7(f)(3)(B).

130. Recent public comments by FTC attorneys indicate that the limitation of private causes of action to Internet Service Providers ("ISPs") may be less restrictive than originally conceived, because the definition of an ISP could include businesses, universities, and other organizations that supply their employees with email access. *See Trade Regulation—E-mail: Definition of "ISP" Under CAN-SPAM Could Permit Legal Actions by Employers*, 72 U.S.L.W. 2696 (May 18, 2004). If this permissive definition is developed, the protection the Act offers to industry against private causes of action may be largely illusory.

131. The per-infraction damages available to ISPs differ from those available to state attorneys general. Under the CAN-SPAM Act, § 7(g)(3), an ISP may recover $100 per violation of section 5(a)(1) (use of false or misleading transmission information), and $25 per violation of any other violation of section 5. For all violations except section 5(a)(1), a statutory damage cap of $1,000,000 is imposed. CAN-SPAM Act, § 7(g)(3)(B). No cap is imposed for use of misleading transmission information. A court may impose treble damages for knowing or willful violation, or if the court determines that the defendant's activity included an aggravated violation under section 5(b), which includes data harvesting or dictionary attacks. *Id.* § 7(g)(3)(C).

attorneys general to bring actions to recover real or statutory damages.[132] The CAN-SPAM Act's only new offering, therefore, is that it includes no private right of action,[133] and imposes a two million dollar recovery cap on the amount that state attorneys general can recover against spammers.[134] Thus, the civil penalties set forth by the Act will not increase the threat of civil enforcement against spammers.

Moreover, the threat of money damages will not deter the worst spammers. Those spammers that are already in violation of federal and state law prohibiting misleading commercial contacts by virtue of misleading header information, subject lines, and sender information are not only cross-border senders, but are undercapitalized such that pursuing fines is not a viable option either for the FTC or state attorneys general. There is no reason to believe that the FTC will be more successful in halting the flood of daily spam received by consumers by virtue of attempting to track down a few spammers per year and impose civil fines than state agencies have been—especially considering that the state agencies were often armed with laws kinder to the agency than is the Act.

Indeed, under the widely celebrated do-not-call list, the FCC has essentially not enforced the law. As of December 18, 2003, the FCC took its first enforcement action against a company—California Pacific Mortgage—for ignoring the do-not-call registry.[135] The action consisted of issuing a citation letter that indicated that continued contact with list registrants could result in monetary penalties.[136] The effect of such a letter on spammers that are, from outside of the United States, hacking computers, using the hacked computers to create a dead end trail for the spam, and then sending fraudulent and misleading spam to millions of recipients daily, will be nil. These spammers have already committed multiple state and federal felonies, and have no resources against which fines could be levied, even if the law could reach them. Thus, the civil penalty provisions of the CAN-SPAM Act serve no purpose against the spammers that the law was intended to stop.

---

132. *See, e.g.*, CAL. BUS. & PROF. CODE § 17529.8 (West 2003).

133. Although this protection is rapidly fading, see *infra* note 138.

134. CAN-SPAM Act § 7(f)(3)(B).

135. *See FCC Takes First Action Under Rules Governing National "Do-Not-Call" Registry*, 72 U.S.L.W. 2368 (Dec. 23, 2003).

136. *Id.* (citing *CPM Funding, Inc.*, DA 03-4026 (Dec. 18, 2003)).

C. An Unexceptionalist Approach to Deterrence Creates Laws Enforced Against the Wrong Parties

The risk of casting broad-reaching jurisdictional nets is that the wrong sort of fish are likely to be caught. The Act's criminal and civil penalties will instead be enforced against legitimate businesses engaged in traditionally-accepted activity that is newly construed to be "commercial" and therefore within the bounds of the prohibitions of the Act. Moreover, the threat against private users is even greater. Although the requirements of the Act—for example, that a sender of an unsolicited commercial email provide a physical address—are easily met by businesses that wish to take prophylactic measures to avoid liability under the act, private users whose emails are deemed commercial will generally not have undertaken those measures. These threats to industry and privacy are discussed in turn.

1. The Threat of the CAN-SPAM Act to Legitimate Businesses: Enforcement Creep and Ineffective Preemption

Jurisdictionally unexceptionalist legislation is not merely harmless. The unenforceability of the law against "true" spammers creates the danger that the laws provisions will be enforced against legitimate businesses that are caught in the interpretive evolution of what content is deemed "commercial." This is the problem of enforcement creep. The danger of enforcement creep is that it penalizes legitimate businesses that already comply with state laws requiring labeling of content. Worse, as legitimate businesses retreat from activities subject to enforcement, enforcement will either have to lapse or expand. The end result of enforcement creep is short-term gains against companies that were not significant offenders to begin with.

Such enforcement creep has, in other contexts, become a bet-the-industry problem. In the junk fax context, a sleeper provision of the Telephone Consumer Protection Act matured after lying dormant for nearly 10 years.[137] The result: complete denial of the fax medium to commercial advertisers,

137. The problem in the Telephone Consumer Protection Act ("TCPA") was caused by a change in the judicial interpretation of whether class actions could be brought under the Act. *See* Nicholson v. Hooters of Augusta, Inc., 95 RCCV 616 (Ga. 2001). This determination contradicted prior decisions on the question and blindsided on the industry. *See* Forman v. Data Transfer, Inc., 164 F.R.D. 400, 405 (E.D. Penn. 1995) (holding that class actions were inconsistent with the personal statutory remedies set forth by the Act). The success of *Hooters* gave rise to a spate of class action TCPA lawsuits that ended the facsimile commercial advertising industry. Missouri *ex rel.* Nixon v. Am. Blast Fax, 323 F.3d 649 (8th Cir. 2003) (rejecting constitutional challenge to the anti-fax portion of the TCPA).

and multiple class action lawsuits, including a $2.2 *trillion* lawsuit filed in California against businesses that advertised using unsolicited faxes.[138] Indeed, the example of the Telephone Consumer Protection Act demonstrates why quickly-passed laws regulating new communications media often err: At the time of the passage of the TCPA, facsimile paper was expensive, and the burdens placed on junk-fax recipients were considerable.[139] However, the same faxes cost much less to receive now, and the statutory damages available under the TCPA are completely disproportionate to the damages actually sustained.[140]

Despite its flaws, the CAN-SPAM Act has avoided the largest source of enforcement creep by attempting to limit private rights of action.[141] Private rights of action generate the greatest potential for enforcement creep because they create incentives for potential plaintiffs to court violations for the purpose of bringing a lawsuit—for example, aggressive posting of email addresses, and failing to use an Internet service with filters—and to expand on the definition of "commercial" contact for purposes of drawing gray-area communications under the rubric of the law.[142] The private incentive to stretch the interpretation of what is "commercial" in an email, or to engage in activity that will attract violations is not present in the law as it exists.[143] However, the Act does require the FTC to prepare a report contemplating a system whereby an individual who provides information leading to a government recovery would receive a quasi-qui tam bounty of up to twenty percent of any amounts recovered.[144] Enforcement creep therefore remains a threat.

The Act also increases the chance that businesses will be subject to differing legal regimes because it incompletely preempts state law in the email context.[145] Prior to the enactment of the CAN-SPAM Act, at least thirty-seven states had already enacted laws regulating the transmission of

---

138. *See Lawsuits Seek 2.2 Trillion over Faxes*, Aug. 23, 2002, *at* http://www.cnn.com/2002/LAW/08/23/junk.faxes.ap/index.html.

139. *See Am. Blast Fax*, 323 F.3d at 656 (evaluating legislative history discussing cost).

140. *But see id.* at 656–60 (concluding that TCPA's means are reasonably tailored to achieve its ends).

141. *But see supra* note 138.

142. *Compare Forman*, 164 F.R.D. at 405, *with Hooters*, No. 95 RCCV at 616 (encouraging and discouraging class actions, respectively).

143. Although, query whether the CAN-SPAM savings clause would operate to save a private right of action for fraud or deception.

144. *See* CAN-SPAM Act § 11 (requiring a report within nine months of the date of enactment that sets forth a "system for rewarding those who supply information about violations of this Act, including—(A) procedures for the Commission to grant a reward of not less than 20 percent of the total civil penalty collected for a violation of this Act . . .").

145. *Id.* § 8.

unsolicited commercial email ("UCE"). State UCE laws set forth a range of solutions to the spam problem, from purely information-forcing to outright prohibition. The best-known state laws were Virginia's anti-spam statute, which made sending misleading email a felony, and California's opt-in statute that purported to govern any electronic mail to or from a California computer if the recipient had not given prior express consent to receipt of the communication.[146]

California's anti-spam statute in particular caught the attention of electronic advertisers, because it prohibited sending email without express prior consent to or from any computer in the state of California.[147] The email marketing industry began to lobby for federal legislation with broad preemptive provisions in an attempt to unseat the California law.[148] The fear among industry members was that the most stringent state law would govern the entire industry, and that businesses would be unable to protect themselves from liability because they could not discern where their advertisements were actually going.[149] For example, if a Yahoo user retrieved his email at a California library, the advertiser would be liable; if the same user retrieved the same email at a library in another state, the advertiser would not be subject to liability. Thus, while the Act and several rival bills were before Congress, the major direct marketing associations lobbied for strong preemption provisions and the exclusion of private rights of action.[150]

---

146. CAL. BUS. & PROF. CODE § 17529 (West 2003); VA. CODE ANN. § 18.2-152.3:1 (Michie 2003).

147. CAL. BUS. & PROF. CODE § 17529–17529.1(b). In an open letter advertisement to Congress in *Roll Call Magazine*, the American Associates of Advertising Agencies, the Association of National Advertisers, and the Direct Marketing Association noted that "[a] new state spam law, effective this January 1, will in effect make it illegal for major news organizations to send advertising-supported email newsletters . . . ." *Congress, Pass National Anti-Spam Legislation NOW or E-Commerce Will Be Crippled!*, ROLL CALL, Nov. 13, 2003 [hereinafter *Pass Legislation NOW*].

148. *See* Stefanie Olsen, *Ad Groups Lobby for Antispam Law*, CNET.COM, *at* http://news.com.com/2100-1024_3-5107059.html (Nov. 13, 2003); *see also Pass Legislation NOW*, *supra* note 147 (promoting the passage of the CAN-SPAM Act).

149. *Pass Legislation NOW*, *supra* note 147 (arguing that "[t]hirty-seven inconsistent state spam laws and proposals for a do-not-email list or [a] labeling [requirement] represent a knee-jerk reaction to the spam crisis" and that "[e]ven minor inconsistencies pose substantial risk to honest businesses, which face large penalties and the threat of class action lawsuits if they violate any state law").

150. *Id.* (noting that "[u]nlike other forms of legitimate commercial communications, e-mail cannot be tailored to avoid state boundaries. Honest businesses cannot possibly comply with all of the laws now on the books"). Indeed, the alternatives were worse, from the industry perspective. Nine bills were introduced with the express purpose of limiting unsolicited commercial email during the 108th Congress. For example, Senator Schumer's Stop Pornography and Abusive Marketing Act proposed *ab initio* a do-not-contact list, did not

The CAN-SPAM Act preempts state laws that purport to control UCE.[151] However, the Act does not preempt state laws to the extent that they prohibit falsity or deception in commercial email.[152] Further, the Act does not preempt the application of general state statutes on fraud or general consumer protection statutes to the email context.[153] The difficulty is that some statutes, including the California statute, define the basic prohibitions in terms of fraud or deception.[154] For example, the California anti-spam statute, most commonly known by its bill number, S.B. 186, included a private cause of action that may survive preemption based on receipt of "deceptive" emails.[155] California S.B. 186 prohibits the sending of an email where a person knows that the email is deceptive.[156] Similarly, Ohio law states that providing false routing information or a false return address is forgery under the Ohio Revised Code.[157] These and other provisions may well survive the general preemption of state law, and subject advertisers to additional risks of liability depending on where the emails are received.[158] Thus, the one protection afforded to industry by the Act—the implied uniformity of regulation created by federal preemption—is illusory. Instead of concerning themselves with just one law, businesses must now worry about fifty-one different sets of rules.

---

contain aggressive preemption provisions, and contained a private consumer right of action. S. 1231, 108th Cong. (2004).

151. CAN-SPAM Act § 8. The preemption provision states:

> (b) STATE LAW.—
>
> (1) IN GENERAL.—This Act supersedes any statute, regulation, or rule of a State or political subdivision of a State that expressly regulates the use of electronic mail to send commercial messages, except to the extent that any such statute, regulation, or rule prohibits falsity or deception in any portion of a commercial electronic mail message or information attached thereto.
>
> (2) STATE LAW NOT SPECIFIC TO ELECTRONIC MAIL.—This Act shall not be construed to preempt the applicability of—
>
> (A) State laws that are not specific to electronic mail, including State trespass, contract, or tort law; or
>
> (B) other State laws to the extent that those laws relate to acts of fraud or computer crime.

Id.

152. *Id.* § 8(b)(2).

153. *Id.* § 8(b)(1)–(2)(B).

154. CAL. BUS. & PROF. CODE § 17529 (West 2003).

155. *See Trade Regulation—Internet Mail: Attorneys Discuss Preemption, Compliance Questions Regarding New CAN-SPAM Act*, 72 U.S.L.W. 2367 (Dec. 23, 2003).

156. *Id.*

157. OHIO REV. CODE ANN. § 2307.64(H), 2913.31 (2003).

158. *See id.*

2. The Threat to Private Users: The Act's Volume-Dependent Distinctions are Insufficient to Distinguish Private Users Subject to Gray-Area Enforcement from Commercial Users

The Act also threatens noncommercial private users. With respect to the enforcement question, I use the term "noncommercial private users" to describe regular Internet users who may be subject to enforcement due to a combination of the wide proscriptive reach of the law and gray areas in the Act's definitions. The definition of what is "commercial" can never be airtight, and private users who send email, later determined to be commercial, risk liability. Thus, the terms "noncommercial private user" and "private user" are used here to describe everyday Internet users who believe they are not subject to the restrictions of the law, but may be wrong.

The problem of separating private users from intrusive spammers is difficult. Given the low cost of the Internet as a data marketing tool, individual people are often behind mass commercial spam operations. Depending on what tools a person uses, and on whether he or she sends many emails, or does so repeatedly, a person can change from a regular Internet user engaged in everyday activity into exactly the type of intrusive commercial spammer the law is intended to prohibit.

To give this problem flesh, imagine the following example. An up-and-coming law professor writes a short book on an emerging issue of law. Feeling that the best way to get his work noticed, and purchased, he emails a "shameless plug" for the book to a regular Internet discussion list, encouraging his colleagues to buy, read, and recommend the book to their students. However, following the general practice of private non-commercial users, the professor does not include his real world address or an opt-out provision as required by the Act. The email is re-sent to all the various members of the listserve. It is not clear whether the professor is subject to enforcement under CAN-SPAM. Certainly the email meets the elements of commercial contact that are proscribed by the statute.[159] The professor may be liable for a per-infraction statutory penalty up to the $2 million cap.[160]

A similar problem is created by private Internet users' participation in viral marketing schemes, which may result in liability under the Act. A common technique among retailers is to provide rewards to private users who recommend a product or service to a friend. In return for a small discount, users earn rewards for the electronic equivalent of word-of-mouth marketing. Viral marketing creates two problems under the Act: the first for

159. CAN-SPAM Act § 3(2)(A) (defining "commercial electronic mail message").
160. *Id.* § 7(f)(3)(A)–(B).

businesses, the second for individual users. First, the Act reaches to the originator of a commercial email for purposes of determining liability. Thus, a marketer who engages in a word-of-mouth campaign may find itself subject to a greatly heightened range of penalties if customers forward email incentives on to friends who have not consented to receive advertisements from that particular marketer.[161] Just as troubling, however, is the potential for liability on the part of private individual users for further downstream sends of the same offer.[162] What began as an attempt to replicate word-of-mouth advertising in an electronic medium thus offers the potential for liability up to the $2 million civil damages limit for private users.[163]

The Act does attempt to draw a line between everyday private users and spammers, but ultimately fails. First, the Act tries to distinguish based on email content: the provisions of the Act only apply to emails that propose or concern a commercial transaction.[164] The Act's definition of "commercial electronic mail message" includes "any electronic mail message [in which] the primary purpose of which is the commercial advertisement or promotion of a commercial product or service (including content on an Internet website operated for a commercial purpose)."[165] This definition does little to exempt everyday Internet users from the prohibitions of the Act. Private non-commercial users regularly exchange emails that could be interpreted as being for the primary purpose of promotion of a commercial product or service. Thus, on a first read, the Act's restricted scope does not protect everyday non-commercial Internet users from liability.

Second, the Act attempts to mitigate the risks of enforcement against private Internet users by tying penalties to the number of emails involved.[166] Presumably, the idea is that because private users send very few emails while spammers send many, the use of a per-infraction standard will insulate private users from at least some of the provisions of the Act. Yet because it is so simple to email a large number of people, the use of a per-infraction standard does little to exempt private users from liability. In fact, a per-infraction standard harms private users more than it helps them. Because the Act uses a per-infraction standard to measure harm, the number of violations, and the liability for those violations, often rises to very high

161. *Id.* § 6(a).
162. *Id.*
163. *Id.* § 7(f)(3)(A)–(B).
164. *Id.* § 3(2)(A).
165. *Id.*
166. *Id.* § 7(f)(3)(A).

numbers.[167] A simple message injudiciously posted to a university listserve—a student attempting to sublet an apartment, for example—could turn a personal proposal for an economic transaction into a multi-million dollar regulatory action against an individual.[168]

Thus, there is not only the risk that legitimate businesses and private individuals will actually suffer unwarranted enforcement. There is also the question of whether the Act will cause both businesses and individuals to refrain from engaging in commercially or personally useful behavior. When a per-infraction measure is used for Internet regulation, the Internet may become too risky to use. When the risk rises high enough,[169] parties will avoid communications that are *probably* legal, but about which there is some question, no matter how slight. While a business may be able to calculate the expected return on a given communication, and thus make a decision as to whether it will engage in an activity as against the percent chance of enforcement for a set dollar amount, the chilling effect is far greater for private users. Individuals are not often repeat players (unless, as above, they are simply commercial spammers in private user clothing), and are not likely to have adequate information to permit them to effectively weigh the consequences of posting an email. The risk of chilling private Internet speech is therefore substantial.

None of the methods contained in the CAN-SPAM Act strongly separate the parties ostensibly protected by the law (private users and legitimate businesses) from the parties the law was meant to target, such as criminal or fraudulent spammers. On the contrary, the primary difference between the two is that it is *more* likely that a private user or legitimate business will be subject to enforcement based on an extended interpretation of what is "commercial" than it is that a criminal spammer will be tracked down and suffer enforcement for activity that squarely falls under the Act's prohibitions. Because jurisdictional unexceptionalism leads to such an

---

167. *See* Andrew Quinn, *U.S. Lawsuits Seek 2.2 Trillion over "Junk" Faxes*, Aug. 23, 2002, *at* http://waw.wardsauto.com/ar/marketing_us_lawsuits_seek. The capacity for per-infraction damages for email violations is far higher.

168. CAN-SPAM Act §§ 3(2)(A), 5, 7(f)(3)(A).

169. The risk for non-fraudulent failures to self-identify is capped at $2 million for action by state attorneys general, and $1 million for a suit by an ISP. *Id.* § 7(f)(3)(B), (g)(3)(B). In sum, then, the criminal and civil penalties set forth by the CAN-SPAM Act threaten the industry and privacy interests they were meant to protect. On the one hand, the provisions of the Act cannot deter spammers because they cannot be enforced. Further, the penalties selected will not deter criminal spammers already in violation of federal and state law, or undercapitalized spammers against whom monetary recovery is not feasible. However, due to the Act's reliance on the "commercial" nature of an email, and its adoption of per-infraction statutory damages, it is likely that the Act will be commonly enforced against legitimate businesses and unwitting private users whose emails are interpreted to fall under the technical definitions of the Act.

impasse, it should be reexamined as an operating assumption for Internet regulations.

V. UNWARRANTED TECHNOLOGICAL EXCEPTIONALISM: EXPERIMENTATION AND OBSOLESCENCE IN THE SELECTION OF NEW RULES OF LAW

Thus far, this article has explored the weaknesses of jurisdictional unexceptionalism. There is another side to the coin: what to do about the actual content of regulations, as opposed to their jurisdictional reach.[170] Should legislators consider the Internet a new medium, and devise new regulations that react to the specific technological features of the Internet ("technological exceptionalism"), or should they first attempt to extend existing principles of law to cover new cases? This section seeks to explore whether there is any intrinsic value in new law governing a new medium. I propose that there is not, and that existing substantive rules governing unsolicited commercial communication can extend well to new cases.

This section will again refer to the CAN-SPAM Act to demonstrate that where Congress has attempted to tie statutory innovation to specific technological features, it has tended to err most deeply. On the other hand, in drafting the CAN-SPAM Act, Congress was most successful when it balanced privacy and commercial interests in a fashion that most closely resembled established jurisprudence governing unsolicited commercial communication.[171]

A. The Act Errs Most Where it Creates Substantive Rules Tied to Specific Technological Features

The hallmark of technological exceptionalism is the drafting of specific laws that refer to the specific technological features. To return to the example of murder, an unexceptionalist approach would apply the murder statute to murders by stone, knife, revolver, or lightsaber.[172] An

---

170. Thus, for example, Jack Goldsmith limits his analysis to the jurisdictional aspects of unexceptionalism, reserving this question. Goldsmith, *supra* note 5, at 1201 ("[The article] does not take a position on the merits of particular regulations beyond their jurisdictional legitimacy.").

171. *See, e.g.*, Martin v. City of Struthers, 319 U.S. 141, 147 (1943) (concluding that where "traditional legal methods" such as permitting a person to hang a "No Solicitation" sign on their door was sufficient, the government was not permitted to enact a blanket ban on door-to-door solicitation).

172. Some commentators have extended this proposition to conclude that there is no separately existing law of the Internet, but merely methods for dealing with the same wrongs committed via different means. *See generally* Easterbrook, *supra* note 46.

exceptionalist law would refer to the technological means by which the deed was accomplished, and tailor the effects of the law to the collateral damage likely to result from a new way of committing a wrong (for example, bank robbery with a machinegun is punished more severely than bank robbery with a water pistol).[173]

Technological exceptionalism creates two problems. The first is the experimentation problem. New solutions are more likely to be wrong simply because they are untried. The doctrine of unintended consequences is very nearly the only constant in law. This principle cannot be taken to extremes, however, because it would bar all new rules. Instead, one ought to measure the quality of legislation not by whether it embodies new rules, but by what measures it takes to avoid getting laws wrong because the consequences have been insufficiently examined. The best method for avoiding unintended consequences is examining what effects those rules have had in similar contexts. Thus, for example, the ability to cherry-pick from good state laws is one of the primary sources of quality in federal law.[174]

The second problem of technological exceptionalism in law is obsolescence. The faster technological features change, the faster the effects of law itself tip from beneficial to, at best, inefficient.[175] Regulating fast-changing technology with laws tied to the specific technological features of the medium can create mismatches between the laws and the industries they are intended to regulate.[176] Again, the problem of obsolescence is not absolute—it would be foolish to avoid all reference to technological features in legislation. However, once again, there are tools that can be used to avoid the obsolescence problem, and the quality of law can be measured by the degree to which it takes advantage of those tools. For example, legislatures might take a page from tax law, and provide sunset provisions for explicitly technological legislation. Or, as is more often the case, the law

173. *See* 18 U.S.C. § 924(c)(7)(A) (2000) (setting forth increased penalties for commission of crimes by means of various firearms).

174. This is not to say that federal law should not innovate; rather that the ability to partially regulate and observe the consequences of law should be fully utilized.

175. See *supra* notes 137–140 and accompanying text for a discussion of the TCPA's anti-fax provisions.

176. A good example is the TCPA's anti-junk-fax provisions, which initially set penalties at a draconian level because of the high cost of specialized facsimile paper. Those facts have changed—faxes are now commonly received, viewed, and deleted in entirely electronic form, and the price of facsimile paper has dropped dramatically. *See supra* notes 139–140 and accompanying text.

might set forth generic standards, and delegate the technological specifics to a technocratic agency better able to adapt with the technology.[177]

The CAN-SPAM Act creates several untested rules tied to specific technological features that are not only at the core of Internet use, but are likely to change as the Internet continues to change. First, the CAN-SPAM Act prohibits the use of a common Internet architecture tool, webcrawling software, in gathering information used to contact customers.[178] "Webcrawling software" is software that organizes information found on Internet websites and usenet newsgroups. When a webcrawler is used to look for potential spammable email addresses, the software searches the Internet for email addresses, and catalogs the addresses for a spammer's use. However, webcrawling software is used for much more than simply gathering email addresses for spam purposes. For example, all of the major search engines use webcrawling software to travel to and catalog the content of websites.

Companies are so concerned with this prohibition that they have begun to abandon the tremendous search capabilities of the Internet. At a December 2003 IAPP teleconference attended by FTC staff attorneys, industry users even questioned whether businesses could legally cut and paste email addresses from a website if they had employees search the Internet by hand.[179] Prohibiting commercial entities from using webcrawling software is counterproductive—webcrawling software can only find information that users have intentionally made public. Thus, it is unclear what privacy interest is being protected at tremendous expense to businesses.

Similarly, the Act imposes restrictions on anonymous registration addresses of email in the hopes of discouraging spammers from the common practice of using anonymously registered addresses to send spam. However, it is also common practice for individual non-commercial users to register anonymous email addresses as a simple means of regenerating net anonymity. Because sites will not register "blank" email addresses, users either enter gibberish, or adopt a *nom de plume*. Either expedient could be considered "misleading" registration information for the purposes of the CAN-SPAM Act, and thus prohibited.[180] Yet these anonymous accounts have significant privacy value for individual non-commercial users. Such users often employ anonymous accounts to subscribe to Internet news

177. I by no means suggest that agency delegation is otherwise a good idea. It may in fact increase the problem, because agencies may be subject to industry capture.

178. CAN-SPAM Act §§ 2(a)(10), 5(b)(1)–(2).

179. *See supra* note 155.

180. CAN-SPAM Act § 4(a)(4).

services, or to receive password access to a site without revealing personal information. The irony is that non-commercial users seeking to register anonymously for privacy purposes usually do not employ the safeguards that permit spammers to register multiple, anonymous accounts without detection.

The Act prohibits filling out more than five email addresses without providing accurate identifying information.[181] However, attempting to stop multiple anonymous or misleading email address registrations by linking the user to the registration—a necessary prerequisite to punishment under the law—is useless. If the ISP could trace and identify spammers who use false information to engage in multiple registrations, it would already have stopped the practice entirely by simply refusing to register the spammers.

Moreover, the rule is unnecessary and is already obsolete. ISPs can stop commercial or quasi-commercial use of anonymously-registered email accounts by limiting private-use account bandwidth to non-commercial levels. There is no reason that Yahoo or AOL must permit a private-use account to send hundreds of thousands of emails. If an account is limited to non-commercial contact levels, the account becomes effectively useless to a mass-spammer. Indeed, some ISPs have already solved the serial anonymous registration problem by using visual or audio "Turing Tests" (tests intended to distinguish between person and machine). This simple expedient requires an entity signing up for the account to enter a password given to them either as part of a warped visual array or a distorted sound file—clear enough to humans, but beyond the perceptual ability of the software used to create serial anonymous sign-ups.

Of course, anonymous accounts limited to non-commercial bandwidth use would still be somewhat useful for spammers seeking to defraud—for example, registering an anonymous email address to send a fraudulent email to a specific target—but not particularly so because the registration of an anonymous email address does nothing to make it harder to trace the registrant. A registrant reveals the computers through which he is connecting to the ISP merely by making the connection and registering the account. Registering the account anonymously makes him no more or less traceable from a technological standpoint. There are certainly ways for an anonymous registrant to hide the trail of computers he or she is using to connect to the registration ISP—such as connecting through a website that strips identifying information to permit true Internet anonymity—but again, it is the use of *those* protections, and not the anonymous email address registration itself, that prevent the spammer from being traced. Thus, the

181. *Id.*

rule against anonymous account registration does not impede spammers, but denies everyday users an important privacy tool.

B. The Act Succeeds Best Where it Follows the Established Contours of Cases Weighing Privacy Rights Against Unsolicited Advertisements

Courts have long weighed personal privacy rights against the right to send unsolicited commercial communications.[182] For Congress to legislate on unsolicited commercial contact that is specifically conducted over the Internet is, to a degree, to reinvent the wheel. At first blush, the body of case law discussing the constitutionality of restrictions on unsolicited commercial contact may not seem useful in an analysis of what legislatures ought to do; i.e., an analysis of the effectiveness—rather than the constitutionality—of laws.[183] Indeed, those cases that evaluate laws limiting unsolicited commercial contact do so primarily under the rubric of free speech analysis.[184] But these free speech cases also contain insights as to how to pragmatically balance privacy and commercial rights. This pragmatism is perhaps the result of constitutional ambiguity: the privacy rights the cases protect are not expressly set forth in the Constitution, and the prohibition on state laws restricting freedom of speech is not clearly defined.[185] Thus, courts have weighed the relative value of the communication and the privacy interests at stake in pragmatic fashion.[186]

What principles can be gleaned from the case law on unsolicited commercial contact that legislatures ought to at least consider in enacting effective Internet laws? It is useful to first scan the rules drawn in the most commonly-cited cases, and then turn to trends that cross cases. Unsolicited commercial speech is treated under the larger umbrella of general

---

182. *See, e.g.*, Bolger v. Youngs Drug Prods. Corp., 463 U.S. 60, 72 (1983); Rowan v. United States Post Office Dep't, 397 U.S. 728, 737 (1970).

183. Other than the fact that legislatures ought not violate the Constitution, whether a law does violate it is often a negotiated meaning between Congress and the courts. Thus, it is not even clear that Congress ought to hamstring itself and apply the canon of constitutional avoidance in its own drafting, since Congress is able to discern for itself where it believes the constitutional line to fall, and may make close calls in its own discretion, subject to review by the courts.

184. Thus, the cases that challenged the federal do-not-call list or the TCPA's anti-commercial fax provisions did so on First Amendment grounds. *See, e.g.*, Missouri *ex rel.* Nixon v. Am. Blast Fax, Inc., 323 F.3d 649, 660 (8th Cir. 2003) (rejecting First Amendment challenge to the TCPA's anti-fax provisions).

185. *See Rowan*, 397 U.S. at 736 ("Without doubt . . . communication is imperative to a healthy social order. But the right of every person 'to be let alone' must be placed in the scales with the right of others to communicate.").

186. *Id.*

commercial speech.[187] Fraudulent commercial speech is immediately recognized as unprotected.[188] The basic rule governing truthful unsolicited advertisements is that "the short, though regular, journey from mail box to trash can . . . is an acceptable burden, at least so far as the Constitution is concerned."[189] Further, the government may not enact a category-wide opt-in measure requiring prior consent to receive communication—at least insofar as political speech is concerned[190]—but may enforce the preference of a recipient to not receive further communications from a given source.[191] And finally, in legislating against unsolicited contact, Congress may differentiate between commercial and noncommercial speech, as long as the distinction relates to the commercial nature of the speech.[192]

Several trends emerge from these cases that might prove useful in selecting rules for Internet regulation. First, the cases generally minimize the permission paradox, that is, any rule that would require a sender to make an unsolicited contact in order to request permission to make another unsolicited contact.[193] This minimization helps parse the cases quite well: although the government cannot require prior express consent to receive categories of communication,[194] a party may request that an individual sender not be permitted to send future communications,[195] because he has read one communication and may generally infer what the sender is likely to say in the future.[196]

Similarly, the case law avoids the "refusal paradox," which is that if a recipient must reject an advertisement based on its content, he must always read the communication (or answer the telephone, or open the email) in order to reject it—which destroys the value of any rejection privilege.[197]

---

187. *Bolger*, 463 U.S. at 72; *see generally* Va. State Bd. of Pharmacy v. Va. Citizens Consumer Council, Inc., 425 U.S. 748 (1976).

188. Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n, 447 U.S. 557, 563 (1980) (protecting only truthful commercial speech).

189. *Bolger*, 463 U.S. at 72 (citing Lamont v. Comm'r of Motor Vehicles, 269 F. Supp. 880, 883 (S.D.N.Y. 1967), *aff'd*, 386 F.2d 449 (2d Cir. 1967), *cert. denied*, 391 U.S. 915 (1968)).

190. Lamont v. Postmaster Gen., 381 U.S. 301 (1965).

191. Rowan v. United States Post Office Dep't, 397 U.S. 728, 731 (1970).

192. City of Cincinnati v. Discovery Network, 507 U.S. 410, 421 (1993); *Cent. Hudson*, 447 U.S. at 562 n.5.

193. *Bolger*, 463 U.S. at 69 n.18; *Lamont*, 381 U.S. at 305.

194. *Lamont*, 381 U.S. at 307. *But see* Missouri *ex rel.* Nixon v. Am. Blast Fax, Inc., 323 F.3d 649, 658–59 (8th Cir. 2003) (requiring prior express consent to send a commercial fax).

195. *Rowan*, 397 U.S. at 737.

196. *Id.* at 738.

197. *Id.* ("The continuing operative effect of a mailing ban once imposed presents no constitutional obstacles; the citizen cannot be put to the burden of determining on repeated occasions whether the offending mailer has altered its material so as to make it acceptable.");

Further, unless the sender is required to identify the unsolicited nature of the commercial communication, the recipient is always at the mercy of the sender, and must receive the next communication or risk missing desired communications.[198] Thus, even though the next communication by a sender might be protected political or religious speech, a recipient can likely rightly refuse the contact based on prior unsolicited and unwanted messages.[199]

Between the permission and refusal paradoxes, a guideline for pragmatic rules governing unsolicited commercial contact emerges: the best rule is the one that minimizes both problems.[200] In the context of unsolicited commercial email, the combination of labeling requirements with ordinary filters follows this guideline. First, to avoid the permission paradox, restrictions on unsolicited commercial email should be opt-out rather than opt-in. But to avoid the refusal paradox, email headers should be clearly labeled as UCE, such that a filter can instantaneously set the email aside if the recipient so desires, not even imposing the costs of junk mail (i.e., the trip from the mailbox to the trash can). The law should facilitate, rather than disturb, the balance point between the ability to communicate and the ability to avoid contact.

Ongoing legislative efforts to create a do-not-email list run the risk of shifting the balance between the permission and refusal paradoxes. A do-not-email list permits recipients to refuse *ab initio* messages from senders they know nothing about that contain true information, the communication of which has been deemed valuable and protected.[201] This article makes no determination as to the constitutionality of such a law,[202] but merely points

---

Martin v. Struthers, 319 U.S. 141, 147–48 (1943) (concluding that although the city is not permitted to ban solicitation entirely, individual citizens could make use of the signs to stop solicitation).

198. *Rowan*, 397 U.S. at 738. For example, if advertisers are permitted to make advertisements look like bills, recipients will be forced to accept the advertisements for fear of missing a bill.

199. *Id.* at 737.

200. This analysis is by no means an exhaustive survey of the pragmatic observations found in the unsolicited commercial speech case law, and these abstractions from case law are certainly not beyond debate. Rather, these examples are meant to demonstrate that significant consideration of the question of unsolicited commercial contact has already been undertaken in the courts, and that there is a set of established jurisprudential tools that legislators might select from in crafting a solution for unsolicited commercial contact conducted via a new medium.

201. Va. State Bd. of Pharmacy v. Va. Citizens Consumer Council, Inc., 425 U.S. 748, 756 (1976).

202. In fact, I believe a do-not-email list is likely a constitutional expression of "the right of every person 'to be let alone,'" *Rowan*, 397 U.S. at 736, but it sets dangerous precedent. If I have an unlimited right to refuse contact on privacy grounds, I may also exercise that right against religious or political speech. If I do indeed have a right to be let alone, the nature of the

out that the further step of a do-not-email list invokes the permission paradox (requiring businesses to make use of other, perhaps more intrusive media to get consumers' attention) and will thus contravene the balance that courts have hammered out between unsolicited commercial speech and privacy.

VI. PATCHING THE CRACKS: EFFECTIVE INTERNET REGULATION THROUGH INCENTIVE, INFORMATION, AND INTERNET ARCHITECTURE CHANGE

Unexceptionalists argue—with some reason—that although obstacles to enforcement and deterrence certainly exist due to the frequency, facility, and cross-border nature of Internet transactions, that is no reason not to pass laws prohibiting Internet wrongs.[203] This argument is true. It would be foolish to give up all hope of deterrence merely because enforcement is hard. Even if laws are minimally enforceable, they may provide some deterrent effect.

There is an important middle ground, however. Laws are not limited to their deterrent effect. Laws can also create incentives and facilitate individual protection of privacy. This section therefore rejects the proposition that the alternative to relying heavily on the deterrent effect of Internet laws is abdication, and discusses several examples of how laws can stop spam by setting incentives and promoting information exchange. For example, laws that provide safe harbors for email advertisers who identify themselves will facilitate filters blocking unsolicited emails. Laws that create incentives for ISPs to adopt Internet architecture changes that actually block spam will similarly stop the spam problem at its source. By focusing on these other roles of law, Internet regulations can vastly simplify the enforcement problem while creating rules that actually block spam.

A. Safe Harbors Permit Easy Filtering of Unsolicited Commercial Email While Focusing Enforcement Resources on Harmful Spam

One solution to the enforceability/deterrence problem is to provide safe harbors for businesses that label their content as commercial and thus facilitate blocking. Instead of requiring businesses to agonize over whether

---

speech does not govern what contacts I can choose to refuse. *See, e.g.*, *Martin*, 319 U.S. at 146–49 (finding no bar under the Constitution to presumptively refuse soliciting call from a Jehovah's Witness by posting a "No Solicitation" sign). This principle, if extended to communication on the Internet, is troubling. Can the government enforce my "right to be let alone" if I express a preference not to be contacted by specific religious or political groups?

203. Goldsmith, *supra* note 5, at 1207–08.

their emails are commercial, noncommercial, or privileged under some prior business relationship exception, a labeling law would simply grant safe harbor from liability or prosecution for any communication as long as the appropriate descriptor was used in the email heading. For example, many state laws have long required businesses to preface commercial communications with "ADV:", or, in the case of pornography, "ADV: ADLT[:]."[204] An additional useful designation could be a label that the email is unsolicited: "UCE:."

In the context of unsolicited commercial email, safe harbors would have two effects.[205] First, safe harbors stop enforcement creep[206] and separate commercial emailers from criminal or fraudulent spammers. Legitimate businesses are willing to state who they are and what they are sending to recipients in order to be freed from the threat of enforcement. Yet self-identification is the one thing spammers are unwilling to do: after all, their relative advantage is a willingness to get past a recipient's filters—both electronic and common-sense—by pretending to be something other than what they are.

Giving companies a safe harbor for emails tagged "UCE" would also directly benefit email recipients. Consumer-grade email filters need only look for the tag and can instantly remove the unsolicited email from the consumer's in-box. This function solves the bulk of all spam problems at the same time that it solves the problem of the costs imposed on recipients in the form of time spent searching through email to avoid unsolicited contacts.

A safe harbor for senders who self-identify also permits enforcement efforts to be focused on spammers who are still willing to violate the law.[207] Annoying, but otherwise harmless, unsolicited commercial emails are filtered out, and can be viewed or refused, at a recipient's option. Those

---

204. *See, e.g.*, ALASKA STAT. § 45.50.479(a) (2003); IND. CODE § 24-5-22-8(1)–(2) (2003); MO. REV. STAT. § 407.1144(2)–(3) (2003).

205. While compliance with the law's requirements may be said to be a "safe harbor," interpretive gray areas, such as a shift in the definition of "commercial email message" threaten legitimate businesses and private users, and cause them to steer clear of commercially and personally useful behavior. A safe harbor, however, grants protection from enforcement once specific positive acts are performed.

206. Safe harbors stop enforcement creep because as long as an email is marked "UCE," the content of the email—be it commercial, transactional, prior business related, or none of the above—simply does not matter.

207. Note that the content of a safe harbor email could still break the law in other respects. An email by a self-identified commercial entity that is marked as unsolicited could still propose a substantive transaction that is fraudulent. But both state and federal laws dealing with fraud still apply in those circumstances, and the task of tracing the defrauding entity is made no more difficult by its compliance with a self-identification safe harbor.

spam emails that remain have been sent by parties willing to break the law to get past a recipient's filters. Enforcement against that subset of email senders has critical advantages. First, there is a greatly reduced risk of enforcement creep because legitimate businesses have been permitted to avoid enforcement by complying with a bright-line self-identification requirement. This system, in turn, permits legislatures to enact much more draconian punishments against spammers without the risk of ensnaring and destroying businesses willing to comply with the law. From the business perspective, because enforcement creep is not an issue (due to the fact that the *sender*, not the enforcing agency, identifies the email as commercial), businesses will not hesitate to engage in activity due to worries that the content of the email might be deemed commercial and thus subject the business to liability.

Second, granting businesses a safe harbor for identifying themselves for filtering purposes hones enforcement and increases the value of reporting violations. ISPs rely on customer-reporting to catch spam. A recipient can mark an email they receive as "spam" and notify the ISP, which then updates its filters to block that message from being forwarded to other users.[208] The CAN-SPAM Act also clearly contemplates that reporting from consumers will play a major role in enforcement.[209] For example, the Act requires the FTC to consider the feasibility of a system granting reporting consumers a bounty on collections made by the government pursuant to information reported to the agency.[210] The value of that reporting rises as consumers deal with less commercial spam—except on a consensual basis by opening their "Bulk Email" folder—and instead report fraudulent spam willing to bypass filters.

In short, the law should not be concerned with spam that can be filtered, but should instead permit the senders of regular unsolicited commercial emails to identify themselves and get out of the enforcement picture. This system would permit a much tighter focus on the fraudulent, often virus-carrying spam sent by parties who are unwilling to self-identify. By relying on the ability of law to create incentives rather than to deter,[211] legislation seeking to limit harmful spam can greatly simplify the problem of enforcement, reduce the risk of ensnaring everyday Internet users with

208. For example, Yahoo uses this system to create an interactive spam filter, a major component of which is using the spam reported by Yahoo account holders to block spam to other Yahoo email accounts. *See generally* Yahoo! Anti-Span Research Center, http://antispam.yahoo.com (last visited Jan. 15, 2005).

209. CAN-SPAM Act § 11.

210. *Id.*

211. Of course, the two are opposite sides of the same coin, but the relative weights granted to each can vary.

penalties intended for criminal spammers, and permit scarce resources to be focused tightly on the type of spam that causes the most harm.

B. Laws Can Also Encourage (or Discourage) Technological Responses That Actually Stop Spam

The best way to stop spam is to adopt technological solutions that make it harder for spammers to fool filters. Laws can either facilitate these technological solutions overtly—by subsidizing the architecture change, or covertly—by discouraging alternatives or constructing legal rules that function as indirect subsidies.

Two brief examples of technology that can reduce spam are active filters and Sender Policy Framework ("SPF") architecture. An active filter is simply password-protected permission to send email to an account. The password can be distributed by automated service, so that the consumer simply instructs his or her system to periodically "update contact authority," and the list of people who can directly contact the user is notified. This permits a user to perform the equivalent of a change of email address without abandoning his electronic real estate.

SPF architecture is an Internet infrastructure solution that changes how ISPs send and receive email, and makes it much more difficult to falsify the origin of an email. The SPF architecture requires each sending domain to post a list of machines that originate messages from that domain. A receiving ISP can then verify that a sender is, in fact, who it says it is. In other words, SPF architecture ties a sender to a specific geographical computer instead of to virtual real estate, making it much harder for a spammer to shift his electronic address every time he engages in another spam attack.

It would be fairly simple to create incentives for ISPs to enable active filters, or to adopt SPF architecture. The funds that would be necessary to create, maintain, and defend a do-not-email list could more profitably be spent educating system administrators, improving the SPF code, and ensuring the widespread adoption of the system. Indeed, it is not clear that additional incentives are needed at all: email users are an audience for the banner advertisements that ISPs sell. Increased privacy attracts email users, thus increasing advertising revenue. The law's best course might be to remain silent, and to permit ISPs to adopt anti-spam measures as a competitive advantage.

Instead of encouraging technological blocks that stop spam, however, the CAN-SPAM Act grants a private right of action for ISPs to recover for

wrongs suffered by their customers.[212] Thus, while the user sustains damage from an email-sent virus, for example, the ISP benefits from statutory per-infraction damages for the spammer's activity.[213] This state of affairs certainly does not create an incentive for ISPs to undertake potentially expensive architecture changes to protect its users, and in fact may undermine the preexisting incentive to do so. The optimal strategy for ISPs under the new law may well be to sue for damages rather than enable active filters or SPF architecture.[214]

In short, legislatures should not abandon deterrence as an objective in regulation, but should explore whether incentives to share information and adopt technological solutions might serve the law's goals more effectively. In the context of unsolicited commercial email, enforcement can be vastly simplified by permitting commercial emailers to separate themselves from true spammers by self-identifying and opting out of the enforcement picture. If technological solutions are adopted that increase the difficulty in falsifying transmission information, spamming becomes even less attractive of an option, because it lessens the comparative advantage of the spammer over the legitimate business that wishes to make a commercial contact.

VII. CONCLUSION

What are the hidden threats of the CAN-SPAM Act? The Act is based on a flawed assumption—that traditional notions of jurisdiction and enforcement will work to govern Internet communications without imposing prohibitive costs on private noncommercial users and legitimate businesses. The Act proposes to concentrate private information in

---

212. CAN-SPAM Act § 7(g).

213. *Id.* The Act does require that the ISP be "adversely affected" by the violation and ties the ISP's actual damages to the "actual monetary loss incurred by the provider." *Id.* § 7(g)(1). But the Act also provides for a statutory recovery of $100 per infraction, up to a $1,000,000 cap. *Id.* § 7(g)(3). Thus, an infraction that primarily damages an ISP's user entitles the ISP to statutory damages of $1,000,000 as long as it adversely affects the ISP in some manner. Moreover, for violations of § 5(a)(1), using false or misleading transmission information, no damages cap is imposed, and damages can be tripled if the court finds the violation was knowing or was an aggravated offense (i.e., was done through a dictionary attack or by using webcrawling software). *Id.* § 7(g)(3)(B), (C)(i)–(ii).

214. One additional problem is that because tracking and enforcing against fraudulent or criminal spammers is difficult and expensive, especially for an ISP building a case for a civil action, ISPs will enforce these rules primarily against the parties about whom they have the most information: legitimate businesses who are willing to comply with the law, but are caught in an expanding definition of what is "commercial" under the Act, or the ISP's own customers. On the other hand, ISPs are quite likely to leave criminal cross-border spoofers and spackers alone for the most part.

government hands, while ignoring the fact that the government is less well-equipped to defend the information than individual citizens. Additionally, the Act limits the use of computer software tools that are the backbone of the information revolution in a manner that harms legitimate businesses, but does not significantly hamper spammers.

The solution is to adopt a different and pragmatic mix of exceptionalist and unexceptionalist approaches to regulating the Internet. While there may be a place for jurisdictional unexceptionalism and content exceptionalism tied to specific technological features in Internet regulation, they are the wrong foundational assumptions. Instead, the legislatures enacting laws regulating the Internet should recognize that there are considerable enforcement difficulties in regulating Internet conduct, and should adopt new strategies to facilitate information exchange and create incentives for Internet architecture changes. On the other hand, legislatures should draw from established principles of law—for example, the "permission paradox" and "refusal paradox" in the unsolicited advertising setting—to balance the right to communicate against the right to be let alone.

Although the Internet has captured the legal imagination for nearly a decade, it is only now that the serious work of regulating communications over this medium has begun. Getting these regulations right is important. The Internet is the first medium to offer the cocktail of instant, frequent, cheap, and cross-border communication in a decentralized architecture. But it will not be the last. The solutions that are developed in response to the challenges posed by Internet regulation will themselves be extended to new communication technologies as they emerge. As they do emerge, what is now "cyberlaw," or the "law of the Internet," will simply become "law"—not because the law will treat the Internet like any other medium, but because emerging media will be treated like the Internet.