

GEORGIA LAW REVIEW

VOLUME 41

FALL 2006

NUMBER 1

ARTICLES

PROTECTING THE INNER ENVIRONMENT: WHAT PRIVACY REGULATION CAN LEARN FROM ENVIRONMENTAL LAW

*Dennis D. Hirsch**

TABLE OF CONTENTS

I. INTRODUCTION 4

* Associate Dean and Professor, Capital University Law School. The author would like to thank the following for their insights about privacy and environmental law and/or their comments on drafts of this Article: Kirk Herath, Benita Kahn, Professors James Beattie, Mark Brown, Alex Cameron, Charles Cohen, Shi-Ling Hsu, Daniel Kobil, Stephen Johnson, J.B. Ruhl, James Salzman, Daniel Solove, Daniel Steinbock, Katherine Strandburg, Peter Swire, Jonathan Weinberg, and the members of the Ohio Legal Scholarship Workshop. He would also like to thank Capital University Law School for supporting the writing of this Article with a summer research grant, and Tiffany Auvdel for the diligent and useful research assistance that she provided.

II.	THE INFORMATION REVOLUTION AND INJURIES TO PRIVACY	11
	A. LEGAL CONCEPTIONS OF PRIVACY	11
	B. THE INFORMATION REVOLUTION	13
	C. THE INFORMATION REVOLUTION AND DAMAGE TO SPATIAL PRIVACY	15
	D. THE INFORMATION REVOLUTION AND DAMAGE TO INFORMATIONAL PRIVACY	17
	1. <i>Computer Profiling</i>	17
	2. <i>Data Mining</i>	18
	3. <i>Data Spills and Identity Theft</i>	19
III.	PRIVACY INJURIES ARE LIKE ENVIRONMENTAL HARMS	23
	A. NEGATIVE EXTERNALITIES	23
	B. THE TRAGEDY OF THE COMMONS	24
	C. SPAM, EXTERNALITIES, AND THE TRAGEDY OF THE COMMONS	25
	D. PERSONAL INFORMATION, EXTERNALITIES, AND THE TRAGEDY OF THE COMMONS	28
IV.	ENVIRONMENTAL LAW AND POLICY AS A MODEL FOR PRIVACY REGULATION	30
	A. COMMAND-AND-CONTROL REGULATION WOULD NOT BE A GOOD FIT FOR THE DIGITAL ECONOMY	33
	B. SECOND GENERATION REGULATION WOULD WORK BETTER	37
V.	USING EMISSION FEES TO REDUCE SPAM	40
	A. AN EMISSION FEE SYSTEM FOR SPAM	43
	B. A NEW PERSPECTIVE ON RECENT PROPOSALS	48
VI.	USING REGULATORY COVENANTS TO PROTECT INFORMATIONAL PRIVACY	50
VII.	USING PUBLIC DISCLOSURE TO PROTECT INFORMATIONAL PRIVACY	57

2006]	<i>PROTECTING THE INNER ENVIRONMENT</i>	3
VIII.	GOVERNMENT SUPPORT FOR ENVIRONMENTAL MANAGEMENT SYSTEMS AS A MODEL FOR IMPROVING THE PROTECTION OF PERSONAL INFORMATION	60
IX.	CONCLUSION	63

“You have zero privacy anyway Get over it.”

*Scott McNealy, Co-founder of Sun Microsystems*¹

WAITRESS: “Well, there’s . . . egg and spam; egg, bacon and spam; egg, bacon, sausage and spam; spam, bacon, sausage and spam; spam, egg, spam, spam, bacon and spam; spam, spam, spam, egg and spam”

MRS. BUN: “Have you got anything without spam in it?”
*Monty Python’s Flying Circus*²

I. INTRODUCTION

Society today is in the midst of an Information Revolution³ that both promises great benefits and ushers in new dangers that require a legal response. Some have sought to convey the significance of what is happening by comparing it to the Industrial Revolution of the early nineteenth century.⁴ That prior transformation brought with it many new technologies, forms of business, goods, services, and other benefits.⁵ Yet, it also generated an unprecedented level of environmental degradation⁶ that far outstripped the ability of the

¹ Polly Sprenger, *Sun on Privacy: ‘Get Over It,’* WIRED NEWS, Jan. 26, 1999, <http://www.wired.com/news/politics/0,1283,17538,00.html>; Sun Microsystems, Sun News—Executive Bios: Scott McNealy (2006), http://www.sun.com/aboutsun/media/ceo/mgt_mcnealy.html.

² 2 GRAHAM CHAPMAN ET AL., *THE COMPLETE MONTY PYTHON’S FLYING CIRCUS ALL THE WORDS* 27 (Pantheon Books 1989). This comedy skit, with its repeated interjections of the word “spam,” is thought to be the source of the term as applied to intrusive and frequent bulk email. See *White Buffalo Ventures, LLC v. Univ. of Tex.*, No. A-03-CA-296-SS, 2004 U.S. Dist. LEXIS 19152, at *2 n.1 (W.D. Tex. Mar. 22, 2004) (explaining this connection).

³ See RICHARD C. TURKINGTON & ANITA L. ALLEN, *PRIVACY LAW* 398 (West Group, 2d ed. 2002) (referring to “[t]he revolution in communications and data processing that is occurring in the United States and much of the world”); Robert E. Litan, *Law and Policy in the Age of the Internet*, 50 *DUKE L.J.* 1045, 1045 (2001) (describing the “Internet revolution”).

⁴ Will Thomas DeVries, *Protecting Privacy in the Digital Age*, 18 *BERKELEY TECH. L.J.* 283, 291 (2003) (“The last generation has seen technological change on a scale matching or exceeding that of the industrial revolution.”); Howard Isenberg, *The Second Industrial Revolution: The Impact of the Information Explosion*, 27 *INDUS. ENG’G.* 14, 15 (1995) (“[H]istorians may very well look back on American business and explain the current industry changes as an Industrial Revolution even more profound than the first one.”); Litan, *supra* note 3, at 1047 (“Some proclaim [the rise of the Internet] to be as important, if not more important, than the Industrial Revolution.”).

⁵ T.K. DERRY & TREVOR I. WILLIAMS, *A SHORT HISTORY OF TECHNOLOGY: FROM THE EARLIEST TIMES TO A.D. 1900*, at 311, 343, 364, 467 (1960).

⁶ See ERIC PEARSON, *ENVIRONMENTAL AND NATURAL RESOURCES LAW* 1–2 (LexisNexis, 2d

existing legal system to deal with it.⁷ Eventually, a new form of law—environmental law—emerged to address these injuries.⁸

Much like the Industrial Revolution, the current Information Revolution is both generating tremendous economic and social benefits and, simultaneously, causing serious and unanticipated damage.⁹ This time, however, the harm is not to the external environment but to an internal one—our privacy.¹⁰ Injuries to privacy are mainly occurring on two fronts: “informational” and “spatial.”

First, new technologies are digitally collecting and tracking our social security numbers, reading habits, political beliefs, health issues, criminal histories, and other pieces of personal information as never before.¹¹ Private businesses are then compiling and analyzing this data to put together comprehensive and invasive pictures of specific individuals.¹² They use these “digital dossiers”¹³ to track our behavior and to market goods and services to us. Our “most intimate information [is being] circulated by an indifferent

ed. 2002) (describing pollution problems caused by Industrial Revolution).

⁷ See ENVIRONMENTAL PROTECTION: LAW AND POLICY 11–12, 23–24 (Robert L. Glickman et al. eds., Aspen Publishers, 4th ed. 2003) (discussing limitations of using nuisance law to attack environmental problems).

⁸ See ENVIRONMENTAL LAW: FROM RESOURCES TO RECOVERY 30–31, 35–40 (Celia Campbell-Mohn et al. eds., West Publ'g 1993) (describing development of federal environmental law).

⁹ Litan, *supra* note 3, at 1045 (“The world is just at the dawn of the Internet revolution, a revolution that promises both benefits and new sets of challenges, if not problems.”).

¹⁰ *Id.* at 1055; see also DANIEL J. SOLOVE ET AL., INFORMATION PRIVACY LAW (2d ed. 2006) (describing these injuries); Pamela Samuelson, *Five Challenges for Regulating the Global Information Society* 9 (2001) (copy on file with author) (discussing threats that computer- and Internet-based technologies pose to privacy).

¹¹ See Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1198–99 (1998) (describing collection, tracking, and use of this data); Pamela Samuelson, *Privacy as Intellectual Property?*, 52 STAN. L. REV. 1125, 1126 (2000) (“The technical infrastructure of cyberspace makes it remarkably simple and inexpensive to collect substantial amounts of information identifiable to particular individuals.”).

¹² See generally Joseph S. Fulda, *Data Mining and Privacy*, 11 ALB. L.J. SCI. & TECH. 105 (2000) (examining use of data mining to analyze individuals’ information); Daniel J. Solove, *Access and Aggregation: Public Records, Privacy, and the Constitution*, 86 MINN. L. REV. 1137 (2002) (advocating increased access and use restrictions on public records and arguing such restrictions are constitutional obligations). Professor Solove notes that “[t]he threat to privacy is not in isolated pieces of information, but in increased access and aggregation, the construction of digital biographies and the uses to which they are put.” Solove, *supra*, at 1218.

¹³ Daniel J. Solove, *Identity Theft, Privacy, and the Architecture of Vulnerability*, 54 HASTINGS L.J. 1227, 1228 (2003).

and faceless infrastructure.”¹⁴ More nefariously, this “faceless infrastructure” employs the data to deny us jobs, credit, insurance, and other social goods, often without our knowledge.¹⁵ Making matters worse, the very fact that so much information is being collected and stored increases the chance that it will fall into the hands of those who would steal our identities to open credit cards, take out mortgages, or do worse in our names.¹⁶ These technological developments inhibit our ability to control our personal information and so injure our “informational privacy.”¹⁷

Second, the new damage to privacy does not end there. We also have a privacy interest in our personal spaces.¹⁸ This right to “spatial” privacy has traditionally protected us from intrusive behavior such as invasions of our homes or telephone calls that “are repeated with such persistence and frequency as to amount to a course of hounding the plaintiff.”¹⁹ Today, the email inbox has become a place of social interaction as important as our living room or phone line. The endless barrage of spam email “hounds” us in this personal space and damages our spatial privacy.

Just as the law had to adapt to changes during the Industrial Revolution, the law today is struggling to address the privacy

¹⁴ DeVries, *supra* note 4, at 298. That individuals do, in fact, find this to be a problem became apparent after the attempt by Lotus Development Corporation and Equifax Corporation to develop a database that would include comprehensive information, such as name, address, marital status, gender, age, type of dwelling, income of household, and purchasing power, of over 100 million individuals in the United States. TURKINGTON & ALLEN, *supra* note 3, at 427. The product, which would have been called “Lotus Marketplace: Households,” was to be made available for a price on CD-ROM. Major public protest met the announcement of this project. Thirty thousand individuals contacted Lotus to indicate that they wanted to be removed from the database. Lotus ultimately decided to abandon the project. *Id.*

¹⁵ See, e.g., Solove, *supra* note 12, at 1151 (revealing how some employers screen potential employees based on personal information they have purchased); Tal Z. Zarsky, “*Mine Your Own Business!*: Making the Case for the Implications of the Data Mining of Personal Information in the Forum of Public Opinion,” 5 YALE J.L. & TECH. 1, 20 (2002–2003) (providing hypothetical in which employer terminates employee based on personal information it has purchased).

¹⁶ Robert O’Harrow, Jr., *Identity Thieves Thrive in Information Age: Rise of Online Data Brokers Makes Criminal Impersonation Easier*, WASH. POST, May 31, 2001, at A1.

¹⁷ See SOLOVE ET AL., *supra* note 10, at 1 (defining information privacy); Kang, *supra* note 11, at 1205 (same).

¹⁸ Kang, *supra* note 11, at 1202 (describing “spatial privacy”).

¹⁹ RESTATEMENT (SECOND) OF TORTS § 652B cmt. d (1977); see also Kang, *supra* note 11, at 1202 (spatial privacy can be invaded by “a car alarm or a telemarketing call”).

damage of the Information Age.²⁰ Many policymakers and legal scholars agree that the existing legal structure is insufficient to deal with the emerging injuries to privacy²¹ and that we need new laws capable of protecting personal privacy in the digital age.²² Rather than reinvent the wheel, they have examined whether existing laws might serve as a model for privacy protection.²³ Legal scholars have argued that the basic principles of property law,²⁴ contract law,²⁵ trade secret law,²⁶ and nuisance law,²⁷ among others, might provide a useful framework on which to base a legal regime to protect privacy. Until now, they have paid far too little attention to environmental law as a model for privacy regulation.²⁸

²⁰ See SOLOVE ET AL., *supra* note 10, at xxvii (identifying central public policy question as extent to which “the law [can] safeguard the right of privacy in an era of rapidly evolving technology”); Samuelson, *supra* note 10, at 9 (stating that preserving privacy is one key policy challenge of the Internet Age).

²¹ See, e.g., DeVries, *supra* note 4, at 306 (“The changes wrought by digital technology, however, are so deep and broad that the old laws and theories are not adapting fast enough.”).

²² See, e.g., Herbert Burkert, *Privacy-Enhancing Technologies: Typology, Critique, Vision*, in TECHNOLOGY AND PRIVACY: THE NEW LANDSCAPE 125, 140 (Philip E. Agre & Marc Rotenberg, eds., 1998) (suggesting rise of information technology presents “challenge for social innovation”).

²³ See Litan, *supra* note 3, at 1047 (stating that rise of Internet has “spawned debate about how, or whether, to translate various legal and policy frameworks familiar in the physical world to the world of ‘cyberspace’ ”).

²⁴ See generally Jacqueline Lipton, *Information Property: Rights and Responsibilities*, 56 FLA. L. REV. 135 (2004) (property law as model).

²⁵ See generally Paul M. Schwartz, *Privacy and the Economics of Personal Health Care Information*, 76 TEX. L. REV. 1 (1997) (contract law as model).

²⁶ See generally Samuelson, *supra* note 11 (trade secret law as model).

²⁷ See generally Adam Mossoff, *Spam–Oy, What a Nuisance!*, 19 BERKELEY TECH. L.J. 625 (2004) (nuisance law as model).

²⁸ Several have applied the environmental analogy to other aspects of the Information Age. For example, one insightful piece has argued that the environmental movement could serve as a model for a political effort to protect the public domain in intellectual property law. James Boyle, *A Politics of Intellectual Property: Environmentalism for the Net?*, 47 DUKE L.J. 87, 87 (1997). Another has used the environmental analogy to shed light on the telecommunications infrastructure. Harmeet Sawhney, *Information Superhighway: Metaphors as Midwives*, 18 MEDIA, CULTURE & SOC’Y 291, 306 (1996). One author has taken the analogy full circle and argued that information policy could be used to generate ideas about how to protect the physical environment. Jim Chen, *Webs of Life: Biodiversity Conservation as a Species of Information Policy*, 89 IOWA L. REV. 495, 501 (2004). In a thoughtful piece, another has argued that privacy injuries are like environmental damage in that they are “general societal problem[s]” rather than “problem[s] of individual concern.” James P. Nehf, *Recognizing the Societal Value in Information Privacy*, 78 WASH. L. REV. 1, 74–81 (2003). The current Article takes the analogy a step further by examining specific environmental policies and how they could be adapted for use in protecting privacy. My research has revealed no

They are overlooking one of the richest and most relevant resources in all of American regulatory law. Over the past forty years, environmental law has been at the epicenter of an intense and productive debate about the most effective way to regulate.²⁹ Initial environmental laws took the form of prescriptive, uniform standards that have come to be known as “command-and-control” regulation.³⁰ These methods, while effective in some settings, proved costly and controversial.³¹ In the decades that followed, governments, academics, environmental and business groups, and others poured tremendous resources into figuring out how to improve upon these methods. This work has produced a “second generation” of environmental regulation, portions of which will be described in detail below.³² Second generation initiatives encourage the regulated parties themselves to choose the means by which they will achieve environmental performance goals.³³ That is what defines them and distinguishes them from first generation regulations under which the agency has the primary decisionmaking power over pollution control methods. This difference tends to make second generation strategies more cost-effective and adaptable than command-and-control rules.³⁴ The proliferation of second generation strategies has led some to identify the environmental field as having “some of the most innovative regulatory instruments in all of American law.”³⁵

other legal scholarship that does this, other than my own brief book chapter, which examined the topic in a preliminary way. Dennis D. Hirsch, *Is Privacy Regulation the Environmental Law of the Information Age?*, in *PRIVACY AND TECHNOLOGIES OF IDENTITY: A CROSS-DISCIPLINARY CONVERSATION* 239, 239–53 (Katherine J. Strandburg & Daniela Stan Raicu eds., 2006).

²⁹ For a summary of the debate with citations to many of the leading sources, see Richard B. Stewart, *A New Generation of Environmental Regulation?*, 29 *CAP. U. L. REV.* 21, 21–24 & n.1 (2001).

³⁰ See JAMES SALZMAN & BARTON H. THOMPSON, *ENVIRONMENTAL LAW AND POLICY* 44 (2003) (describing “command-and-control” regulation); Dennis D. Hirsch, *Symposium Introduction: Second Generation Policy and the New Economy*, 29 *CAP. U. L. REV.* 1, 1–2 (2001) (same).

³¹ For various critiques, see Hirsch, *supra* note 30, at 2–5; Stewart, *supra* note 29, at 21–22.

³² See *infra* notes 223–356 and accompanying text.

³³ See *infra* notes 207–12 and accompanying text.

³⁴ See *infra* notes 213–17 and accompanying text.

³⁵ SALZMAN & THOMPSON, *supra* note 30, at 41.

Privacy regulation today finds itself in a debate similar to the one that the environmental field has been engaged in for years. On the one hand, there is a growing sense that the digital age is causing unprecedented damage to privacy and that action must be taken immediately to mitigate these injuries.³⁶ On the other, a chorus of voices warns against the dangers of imposing intrusive and costly regulation on the emerging business sectors of the information economy.³⁷ Missing thus far from the dialogue is any significant

³⁶ See *Developments in the Law—The Law of Cyberspace*, 112 HARV. L. REV. 1574, 1581 (1999) (discussing “calls for regulation and governance” of Internet); Samuelson, *supra* note 10, at 10 (commentators believe that “law will have to play a role” in solving cyberspace privacy problem). See generally SOLOVE ET AL., *supra* note 10, at 39–59 (describing scholarship on value of privacy); Litan, *supra* note 3, at 1058 (citing Harris survey finding that 92% of consumers are “concerned” and 67% are “very concerned” about misuse of their personal data online); Joel R. Reidenberg, *Restoring Americans’ Privacy in Electronic Commerce*, 14 BERKELEY TECH. L.J. 771 (1999) (arguing electronic commerce has resulted in need for new legal framework to protect privacy).

There are some who dispute the importance of privacy as a societal value. For example, Judge Richard Posner has argued that privacy allows individuals to selectively disclose only certain facts about themselves and so to manipulate others’ perceptions of them. Richard A. Posner, *The Right to Privacy*, 12 GA. L. REV. 393, 395 (1978). Due to such concealment, people engage in “disadvantageous transactions” with these individuals that they would avoid if they had more complete information about them. *Id.* Posner believes that, in some instances, society would benefit from less privacy rather than more. *Id.* at 402–03. Others have critiqued privacy from a communitarian perspective, see, e.g., AMITAI ETZIONI, *THE LIMITS OF PRIVACY* (2000), or from a feminist one, see, e.g., Reva B. Siegel, “*The Rule of Love*”: *Wife Beating as Prerogative and Privacy*, 105 YALE L.J. 2117 (1996).

The fact that some privacy injuries are contested may make them more analogous to pollution (or resource exploitation) that damages the environment itself, than to pollution that injures human health. Activities that damage the environment itself—for example, drilling for oil in the Arctic or mining a pristine landscape—are often contested in much the same way that privacy injuries are. Many view such activities as harmful. Yet some dispute the underlying value judgment and see only benefits from turning the environment to a more productive use. Environmental pollution that causes damage to human health, on the other hand, is far less contested. No one would seriously argue that more pollution of this type benefits society (although some may dispute the seriousness of the damage or whether the economic benefits outweigh it). This complicates the analogy between privacy impacts (which are contested) and injuries to public health (which are not). I am grateful to Professor Solove for pointing this out.

³⁷ TURKINGTON & ALLEN, *supra* note 3, at 428 (demonstrating that polls show public does not want regulation to constrain information economy); Jay P. Kesan, *Private Internet Governance*, 35 LOY. U. CHI. L.J. 87, 94 (2003) (discussing how debate over top-down versus bottom-up regulation has led both government and private industry to “prefer self-regulation”); Litan, *supra* note 3, at 1045 (stating that in regulating the Internet, “policymakers’ first instinct should be to rely on markets and technology to address troublesome issues”); Paul M. Schwartz, *Internet Privacy and the State*, 32 CONN. L. REV. 815, 848 (2000) (noting current policy rhetoric insists that “[t]he market, bottom-up, and industry self-regulation are to be the essential elements of any solution”).

discussion of the more flexible “second generation” regulatory strategies that might be able to bridge this gap. It took environmental law decades to arrive at these alternatives. The privacy field could capitalize on this experience by looking to these environmental policies as models for privacy regulation.³⁸

This Article argues that second generation environmental laws and policies can serve as a model for protecting privacy in the Digital Age. In so doing, this Article fills a gap in existing privacy law scholarship, which has not made full use of the environmental experience. Part II describes the Information Revolution and the tremendous damage that it is causing to privacy.³⁹ It considers both the ways in which the increased collection and use of personal information injures informational privacy, and the ways in which the spammers’ daily assault on our inboxes erodes our spatial privacy. Part III refines the analogy between privacy injuries and environmental damage in order to reveal the common conceptual structure that links them.⁴⁰ Like smokestack industries that produce environmental pollution, digital economy businesses often do not bear the cost of the harms that they inflict. Privacy injuries, much like environmental damage, accordingly qualify as “negative externalities.”⁴¹ If left unchecked, these privacy-infringing industries will ultimately destroy the very resources on which they themselves depend. This will generate the same kind of “tragedy of the commons” that environmental laws were designed to alleviate.⁴²

Parts IV through VIII turn to the specific lessons that privacy regulation might draw from environmental law. Part IV describes in greater detail the evolution in environmental regulation from first generation “command-and-control” regulation to more flexible second generation instruments.⁴³ It argues that command-and-control type regulations would not be a good fit for the highly diverse and dynamic digital economy but that second generation regulations show great promise. Part V draws on a particular second generation

³⁸ See *infra* notes 175–80 and accompanying text.

³⁹ See *infra* notes 48–134 and accompanying text.

⁴⁰ See *infra* notes 135–69 and accompanying text.

⁴¹ See *infra* notes 135–38 and accompanying text.

⁴² See *infra* notes 140–43 and accompanying text.

⁴³ See *infra* notes 170–222 and accompanying text.

environmental strategy—emission fees—and shows how it could readily be adapted for the purpose of reducing spam.⁴⁴ Parts VI, VII, and VIII explain how several other innovative environmental approaches—regulatory covenants, pollution release and transfer registries, and government support for environmental management systems—could be adapted for the privacy field and used to protect personal information in the digital age.⁴⁵ Ultimately, the Article concludes that by building on the well-developed foundation of environmental regulation, we can achieve targeted laws that protect privacy without strangling technological innovation. Thus, we need not “get over” our desire for privacy as the opening quote suggests,⁴⁶ and in the words of Mrs. Bun, we can indeed have our “eggs” without so much spam in them.⁴⁷

II. THE INFORMATION REVOLUTION AND INJURIES TO PRIVACY

What is “privacy” from a legal and regulatory point of view? What is the Information Revolution, and how is it causing damage to privacy? We turn first to these questions.

A. LEGAL CONCEPTIONS OF PRIVACY

Louis Brandeis and Samuel Warren, in their classic article *The Right to Privacy*, initiated serious legal thinking about privacy.⁴⁸ They focused on common law decisions protecting against invasions of the personal realm⁴⁹ and grouped them into a new category—the “right to privacy”⁵⁰—the invasion of which was a tort.⁵¹ They described privacy as the right to protect one’s “inviolate personality”

⁴⁴ See *infra* notes 223–82 and accompanying text.

⁴⁵ See *infra* notes 283–356 and accompanying text.

⁴⁶ See *supra* note 1 and accompanying text.

⁴⁷ See *supra* note 2 and accompanying text.

⁴⁸ See generally Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890) (suggesting remedies for invasion of privacy). See also Kathleen M. Sullivan & Gerald Gunther, CONSTITUTIONAL LAW 1069 (Robert C. Clark et al. eds., Foundation Press 15th ed. 2004) (noting significance of Warren and Brandeis article).

⁴⁹ Warren & Brandeis, *supra* note 48, at 201–13 & n.1.

⁵⁰ *Id.* at 213.

⁵¹ *Id.* at 219.

against unwarranted intrusion or revelation,⁵² or more famously, as the “right of the individual to be let alone.”⁵³ From this root, three primary branches of privacy law have grown: spatial privacy, decisional privacy, and informational privacy.⁵⁴ Spatial privacy protects personal spaces against an “invasion by unwanted objects or signals.”⁵⁵ Where the federal government is the intruder, the right is based in the Fourth Amendment.⁵⁶ Where a private party is the intruder, it is based on common law tort doctrines.⁵⁷ For example, the tort of “intrusion upon seclusion” exists where one “intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns.”⁵⁸ This includes physical invasions, such as when one enters the home of another without permission.⁵⁹ It also includes intrusive behavior such as when “telephone calls are repeated with such persistence and frequency as to amount to a course of hounding the plaintiff, that becomes a substantial burden to his existence.”⁶⁰ In either case, the person is subjected to “territorial overcrowding.”⁶¹

The decisional privacy cases, most of which are grounded in the Constitution, guard an individual’s right to make certain “self-defining choices without state interference.”⁶² These cases limit government intrusion into intimate decisions such as whether to use birth control⁶³ or obtain an abortion.⁶⁴ This body of privacy law is

⁵² *Id.* at 205; DeVries, *supra* note 4, at 286.

⁵³ Warren & Brandeis, *supra* note 48, at 205.

⁵⁴ See Kang, *supra* note 11, at 1202, for helpful and clear discussion dividing privacy rights into three clusters: “Space, Decision, and Information.”

⁵⁵ *Id.*

⁵⁶ See, e.g., *Kyllo v. United States*, 533 U.S. 27, 40 (2001) (holding that Government cannot use thermal imaging equipment to monitor movement through walls of house without search warrant).

⁵⁷ See, e.g., RESTATEMENT (SECOND) OF TORTS §§ 652A–652E (1977) (identifying four such torts: (1) intrusion upon seclusion, (2) appropriation of name or likeness, (3) publicity given to private life, and (4) publicity placing person in false light).

⁵⁸ *Id.* § 652B.

⁵⁹ *Id.* § 652B cmt. b.

⁶⁰ *Id.* § 652B cmt. d; see also Kang, *supra* note 11, at 1202 (explaining that spatial privacy can be invaded by “a car alarm or a telemarketing call”).

⁶¹ Kang, *supra* note 11, at 1202.

⁶² *Id.* at 1203.

⁶³ See generally *Griswold v. Connecticut*, 381 U.S. 479 (1965) (discussing privacy right in context of contraception).

⁶⁴ *Roe v. Wade*, 410 U.S. 113, 153 (1973); see also DeVries, *supra* note 4, at 287 (discussing

“principally concerned with choice, an individual’s ability to make certain significant decisions without interference.”⁶⁵

Informational privacy refers to the right to control the “collection, use, and disclosure” of one’s personal information.⁶⁶ This body of law, which draws on the Constitution, statutes, the common law, and international law,⁶⁷ protects against the improper dissemination of intimate or confidential information in ways that would embarrass or otherwise compromise the individual concerned. For example, it protects against inappropriate disclosure of sensitive medical information that could be used to the person’s detriment.⁶⁸ It is “ ‘an individual’s claim to control the terms under which personal information—information identifiable to that individual—is acquired, disclosed, and used.’ ”⁶⁹ As described below, the Information Revolution primarily damages spatial and informational privacy.

B. THE INFORMATION REVOLUTION

The defining feature of the Information Revolution is the shift from analog to digital technology for storing, manipulating, and transferring information.⁷⁰ This core development has transformed the fields of communications and data processing. With respect to

privacy in context of “state intrusion upon certain intimate decisions”).

⁶⁵ Kang, *supra* note 11, at 1202.

⁶⁶ SOLOVE ET AL., *supra* note 10, at 1; accord TURKINGTON & ALLEN, *supra* note 3, at 77 (discussing “informational privacy”); Robert W. Hahn & Anne Layne-Farrar, *The Benefits and Costs of Online Privacy Legislation* (AEI-Brookings Joint Ctr. for Regulatory Studies, Working Paper No. 01-14, 2001), available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=292649 (stating that most definitions of privacy “include a person’s ‘right’ to his or her own information”); Kang, *supra* note 11, at 1204 (“[I]nformation privacy concerns an individual’s control over the processing – i.e. the acquisition, disclosure, and use – of personal information.”).

⁶⁷ SOLOVE ET AL., *supra* note 10, at 2. For a description of this body of law, see generally *id.* and TURKINGTON & ALLEN, *supra* note 3, at 77–294.

⁶⁸ Kang, *supra* note 11, at 1203.

⁶⁹ *Id.* at 1205 (citing INFO. INFRASTRUCTURE TASK FORCE, *PRIVACY AND THE NATIONAL INFORMATION INFRASTRUCTURE: PRINCIPLES FOR PROVIDING AND USING PERSONAL INFORMATION* (1995), available at <http://nsi.org/Library/Comm/niiprivp.htm>).

⁷⁰ TURKINGTON & ALLEN, *supra* note 3, at 399; see also HENRY H. PERRITT, JR., *LAW AND THE INFORMATION SUPERHIGHWAY 27* (2d ed., Aspen Law & Bus. 2001) (1996) (“The move from analog to digital technologies for storing and transmitting information is the foundational shift in technology.”).

communications, digitization allows users to transfer information with amazing ease, accuracy, and speed. It also permits users to more easily share information with a large number of recipients (e.g., sending an email blast to a thousand recipients). These developments depend not just on the digitization but also on the infrastructure that has arisen to accommodate it. This infrastructure may be as simple as an office computer network,⁷¹ or it may be as all-encompassing as the Internet—the international “network of networks”—which links networks and computers around the globe and allows them to transfer data to one another.⁷² The existence of the Internet enables applications such as email. It also makes possible the World Wide Web—the millions of websites and web pages that users can access with the help of a “browser.”⁷³ These technologies and applications have transformed the way we communicate.

The Information Revolution has also profoundly changed the collection, aggregation, and processing of data.⁷⁴ Transactions today do not generate a paper receipt but instead generate a digital record that is often traceable to the individual.⁷⁵ As a consequence, digital “[r]ecords exist of our physical health, workday performances, telephone calls, use of credit, and cyberspace behavior.”⁷⁶ In an analog world, these records would have been stored away in file cabinets or boxes making it almost impossible to compile them.⁷⁷ Digitization makes this task inexpensive and fast.⁷⁸ Computers can sort and match this data instantaneously⁷⁹ and so compile

⁷¹ See PERRITT, *supra* note 70, at 4 (discussing different networks and how they work).

⁷² See *id.* at 5 (calling Internet “the archetypal open network”); see also TURKINGTON & ALLEN, *supra* note 3, at 398 (defining the Internet as “an internationally linked system of computer networks on which the data flows”).

⁷³ See PERRITT, *supra* note 70, at 9–11 (defining and discussing World Wide Web and browser).

⁷⁴ DeVries, *supra* note 4, at 291; Samuelson, *supra* note 11, at 1126; see also TURKINGTON & ALLEN, *supra* note 3, at 399 (“Digital technology has tremendously increased the capacity for data acquisition.”).

⁷⁵ DeVries, *supra* note 4, at 292.

⁷⁶ Schwartz, *supra* note 25, at 17.

⁷⁷ DeVries, *supra* note 4, at 301.

⁷⁸ Samuelson, *supra* note 11, at 1126 (“Once these data have been collected, information technologies make it very easy and cheap to process the data in any number of ways (for example, to make profiles of particular users’ interests).”).

⁷⁹ TURKINGTON & ALLEN, *supra* note 3, at 399 (“Once records have become computerized,

information about an individual. When these developments are linked to those in communications, the results are staggering. Information can not only be aggregated and analyzed, it can be transported quickly over the Internet to one or many recipients. This, in turn, is creating new injuries to privacy.

C. THE INFORMATION REVOLUTION AND DAMAGE TO SPATIAL PRIVACY

Spatial privacy protects against intrusions such as unauthorized entry into one's home or repeated and annoying telephone calls.⁸⁰ Today, the email "inbox" is a personal space as significant as the living room or phone line. When someone substantially intrudes upon this space to the extent that we feel bothered and burdened, the intruder violates our "right to be let alone"⁸¹ in much the same way as if someone were harassing us with "persisten[t]" and "frequen[t]" telephone calls to our home.⁸² Today, spatial privacy includes "the right to refuse unwanted email or online solicitations."⁸³

It follows that spam—"the massive amount of unsolicited commercial e-mail . . . that is sent out each day across the Internet and into inboxes everywhere"⁸⁴—is not only an annoyance; it is also a substantial burden that invades our spatial privacy. Single spammers send from 50 to 250 million emails per day.⁸⁵ The total

unprecedented capacity to acquire data occurs through the matching of computerized records."); Neil Weinstock Netanel, *Cyberspace Self-Governance: A Skeptical View from Liberal Democratic Theory*, 88 CAL. L. REV. 395, 474 (2000) ("It is not merely that seemingly infinite amounts of information can be collected and permanently stored. Digital information processing also entails aggregating previously scattered bits of information from different contexts. It thus produces virtually limitless possibilities for compiling, analyzing, and systematizing such information.")

⁸⁰ See RESTATEMENT (SECOND) OF TORTS § 652B cmt. d (1977) (discussing interference with seclusion); Kang, *supra* note 11, at 1202 (noting spatial privacy can be invaded by "a car alarm or a telemarketing call").

⁸¹ See *supra* notes 49–53 and accompanying text.

⁸² RESTATEMENT (SECOND) OF TORTS § 652B cmt. d.

⁸³ Hahn & Layne-Farrar, *supra* note 66, at 2.

⁸⁴ Mossoff, *supra* note 27, at 626–27; see also AMERICAN HERITAGE DICTIONARY (4th ed. 2000), available at <http://dictionary.reference.com/search?q=spam> (defining "spam" as "[u]nsolicited e-mail, often of a commercial nature, sent indiscriminately to multiple mailing lists, individuals, or newsgroups; junk e-mail").

⁸⁵ Mossoff, *supra* note 27, at 632.

number of spam messages has jumped from 140 billion in 2001⁸⁶ to 2 trillion in 2004.⁸⁷ This onslaught forces the average American to spend fifteen hours per year deleting spam,⁸⁸ to spend money on filters to reduce it,⁸⁹ and to overlook or inadvertently delete desired email, “thus reducing the reliability and usefulness of electronic mail to the recipient.”⁹⁰ Internet Service Providers (ISPs) incur further costs from spam⁹¹ that they often pass on to their customers.⁹² In addition, children can inadvertently access pornographic spam.⁹³ These costs have led the Senate to conclude that spam is “one of the most pervasive intrusions in the lives of Americans.”⁹⁴ We can conceptualize this intrusion as a trampling of our right to be let alone, an invasion of our spatial privacy.

D. THE INFORMATION REVOLUTION AND DAMAGE TO INFORMATIONAL PRIVACY

⁸⁶ *Id.* at 627.

⁸⁷ Lily Zhang, *The CAN-SPAM Act: An Insufficient Response to the Growing Spam Problem*, 20 BERKELEY TECH. L.J. 301, 304 (2005).

⁸⁸ NewsNet5.com, *Deleting Spam Takes up a Lot of Time at Work*, Sept. 14, 2003, <http://www.newsnet5.com/print/2455591/detail.html>; *see also* Zhang, *supra* note 87, at 305 (noting spam recipients must spend “considerable amounts of time” deleting spam email). Recipients “may also have to pay for additional disk space for their e-mail accounts” in order to handle the quantity of spam messages. Zhang, *supra* note 87, at 305. In addition, Americans who still use a dial-up modem to access their email accounts must pay by the minute for the privilege (some at long-distance rates). S. REP. NO. 108-102, at 7 (2003), *as reprinted in* 2004 U.S.C.C.A.N. 2348, 2353. This means that the effort spent downloading, reviewing, and deleting spam costs them not only time but also money on their phone bill. *Id.*; *see also* CAN-SPAM Act of 2003, 15 U.S.C.A. § 7701(a)(3) (West 2003) (finding that consumers incur costs for “the time spent accessing, reviewing, and discarding” spam).

⁸⁹ Zhang, *supra* note 87, at 306. The more effective filters are often provided at a cost of thirty to forty dollars. *Id.*

⁹⁰ 15 U.S.C.A. § 7701(a)(4) (congressional finding); Zhang, *supra* note 87, at 307; *see also* Saul Hansell, *Postage Due, with Special Delivery, for Companies Sending E-Mail to AOL and Yahoo*, N.Y. TIMES, Feb. 5, 2006, § 1, at 25 (citing study showing that Internet Service Provider filters inadvertently capture 20% of legitimate email).

⁹¹ Zhang, *supra* note 87, at 305–06 (noting further costs of installing filters, expanding bandwidth, and hiring staff to deal with spam-related complaints).

⁹² S. REP. NO. 108-102, at 6. A 2001 study found that spam costs Internet subscribers worldwide \$9.4 billion each year. *Id.*

⁹³ 15 U.S.C. § 7701(a)(5) (congressional finding).

⁹⁴ S. REP. NO. 108-102, at 2.

The Information Revolution is harming informational privacy through (1) the collection of clickstream data to construct computer profiles of individual Internet users,⁹⁵ (2) increased aggregation and analysis of personal information through the practice of data mining,⁹⁶ and (3) increased breaches in data security that augment the risk of identity theft.⁹⁷

1. *Computer Profiling.* Moving through cyberspace generates far more records than similar journeys through real space does. Each web page that we visit, each query that we make, is “dutifully recorded, sorted, saved, and exchanged by computers.”⁹⁸ This “clickstream” data can be of great commercial value.⁹⁹ Technologies have accordingly been designed to assist with tracking it. For example, many websites place “cookies” on the hard drives of their visitors,¹⁰⁰ which tell the site when that particular user has returned¹⁰¹ and track how that individual makes use of the site.¹⁰² Internet advertising services and data mining companies collect this information from many sites,¹⁰³ allowing them to put together a comprehensive profile of where an individual user has traveled on the Web and what he or she has done there.¹⁰⁴ This “computer

⁹⁵ For a good description of how this occurs, see Kang, *supra* note 11, at 1223–32.

⁹⁶ See generally Fulda, *supra* note 12 (discussing data mining process); Solove, *supra* note 12 (discussing formation of digital biographies from public records information).

⁹⁷ See Solove, *supra* note 13, at 1245 (suggesting problem of identity theft stems, in part, from fact that “we are becoming a society increasingly dependent upon personal information”).

⁹⁸ Kang, *supra* note 11, at 1198; see also Samuelson, *supra* note 11, at 1126 (“The technical infrastructure of cyberspace makes it remarkably simple and inexpensive to collect substantial amounts of information identifiable to particular individuals.”).

⁹⁹ DeVries, *supra* note 4, at 292 n.68; see also Schwartz, *supra* note 37, at 818 (describing how “[t]he private sector currently captures and makes commercial use of personal information on the Internet”).

¹⁰⁰ Kang, *supra* note 11, at 1227.

¹⁰¹ SOLOVE ET AL., *supra* note 10, at 624–26. One purpose behind this is to allow the website to better welcome back that user the next time. See, e.g., Kang, *supra* note 11, at 1227 (“[B]y accessing the cookie, the server can automatically present local movie features without querying the user for her location.”).

¹⁰² JANLORI GOLDMAN ET AL., PRIVACY: REPORT ON THE PRIVACY POLICIES AND PRACTICES OF HEALTH WEB SITES 27 (2000).

¹⁰³ Kang, *supra* note 11, at 1228–29; see also Litan, *supra* note 3, at 1058 (discussing “cookies”).

¹⁰⁴ Kang, *supra* note 11, at 1228 & n.148. DoubleClick, a major Internet advertising agency, possesses information on the surfing habits of 100 million users generated in this way. TURKINGTON & ALLEN, *supra* note 3, at 458–60; Daniel Tynan, *Privacy 2000: Should You Trust the Web?*, CNN.COM, May 24, 2000, <http://archives.cnn.com/2000/TECH/computing/>

profile” may contain sensitive information regarding political beliefs, sexual orientation, health issues, or other personal topics.¹⁰⁵

2. *Data Mining.* Data mining companies, also called data “brokers,” purchase computer profiles and combine them with information gathered from public records, the media, credit reporting agencies, private investigators, and other sources.¹⁰⁶ They draw out the information about specific individuals.¹⁰⁷ They then “mine” this data to infer even more about that person.¹⁰⁸ “Mining” of data differs from the standard use of a database. Generally, a query to a database returns sought-after information that is explicit in that database.¹⁰⁹ For example, if an individual searches for a particular name and address in a database of “contacts,” the search will return a name and address. Data mining seeks relationships or patterns that allow the data miner to infer additional, latent information about the individual.¹¹⁰ For example, it might use a home address and purchasing habits to infer a person’s political party. It could then sell that information to a political campaign. The issue “is not merely that seemingly infinite amounts of information can be collected and permanently stored. Digital information processing also entails aggregating previously scattered bits of information from different contexts. It thus produces

05/24/privacy.2000.idg.

¹⁰⁵ See Kang, *supra* note 11, at 1199 (noting “extensive data collection takes place as we travel through other cyberspace domains . . . to research health issues and politics; to communicate to individuals, private institutions, and the state; and to pay our bills and manage our finances”).

¹⁰⁶ DeVries, *supra* note 4, at 301; see also Solove, *supra* note 12, at 1141 (stating that “much of the personal information contained in public records . . . is relatively innocuous” but “aggregated together” presents a problem).

¹⁰⁷ The largest of them possess personal information on hundreds of millions of Americans. For example, Acxiom, a large data broker, possesses information on almost every adult in the United States. SOLOVE ET AL., *supra* note 10, at 629 (quoting ROBERT O’HARROW, JR., NO PLACE TO HIDE 34 (2005)). Acxiom’s profile can include name, age, address, income, marital status, occupation, religion, ethnicity, make and price of car, reading habits, and many other pieces of information. *Id.* at 37–50. ChoicePoint, another large data broker, also has records on virtually every adult in America. Grant Gross, *ChoicePoint’s Error Sparks Talk of ID Theft Law*, PC WORLD, Feb. 23, 2005, www.PCworld.com/article/id,119790-page,1/article.html. It has access to about 19 billion public records. *Id.*

¹⁰⁸ This process is also referred to as “knowledge discovery in databases” or KDD. Zarsky, *supra* note 15, at 4.

¹⁰⁹ Fulda, *supra* note 12, at 106.

¹¹⁰ *Id.*

virtually limitless possibilities for compiling, analyzing, and systematizing such information.”¹¹¹

3. *Data Spills and Identity Theft.* The increased digitization and aggregation of large amounts of personal information enhance the likelihood that it will become wrongfully appropriated and misused.¹¹² The year 2005 alone witnessed fifty data security breaches involving the personal information of more than fifty million individuals.¹¹³ Those in the industry, with a nod to the environmental analogy, refer to these breaches as “data spills.”¹¹⁴ Such releases contribute to identity theft,¹¹⁵ where someone wrongfully obtains another’s personal data and “uses it to open new bank accounts, acquire credit cards, and obtain loans in that individual’s name.”¹¹⁶ The average victim of identity theft spends 330 hours clearing her name¹¹⁷ and suffers damage to her credit

¹¹¹ Netanel, *supra* note 79, at 474; *see also* DeVries, *supra* note 4, at 307–08 (“The underlying problem of informational privacy in the digital age is the ability to access and aggregate vast amounts of otherwise harmless personal data into a form that can do real damage to the individual’s sense of self-determination and autonomy.”).

¹¹² *See, e.g.*, Robert O’Harrow, Jr., *Identity Thieves Thrive in Information Age: Rise of Online Data Brokers Makes Criminal Impersonation Easier*, WASH. POST, May 31, 2001, at A1 (“[R]eports available from hundreds of brokers on the World Wide Web can serve as Information Age keys in the hands of criminals.”).

¹¹³ SOLOVE ET AL., *supra* note 10, at 700. For example, in March 2005, LexisNexis reported that hackers had stolen information on 32,000 people that included social security numbers, drivers licenses, and other personal data. Paul Roberts, *Hackers Grab LexisNexis Info on 32,000 People*, PC WORLD, Mar. 9, 2005, <http://www.pcworld.com/article/id,119953/article.html>. ChoicePoint, another major data broker, reported that it had mistakenly sold 145,000 individuals’ personal information to identity thieves posing as legitimate businesspersons. *Id.* CitiFinancial announced that it had lost unencrypted data tapes containing personal information on nearly 4 million customers. Karen L. Werner, *CitiFinancial to Encrypt Data in Wake of Breach Affecting 3.9 Million Customers*, 4 Privacy & Sec. L. Rep. (BNA) 756, 756 (June 13, 2005). CardSystems, a processor of credit card transactions, reported that hackers entered its system and may have extracted the names, account numbers, and security codes of millions of consumers. Eric Dash & Tom Zeller, Jr., *Mastercard Says 40 Million Files Are Put at Risk*, N.Y. TIMES, June 18, 2005, at A1.

¹¹⁴ *See, e.g.*, Brett Glass, *Tower Records Suffers Massive Data Spill*, EXTREME TECH, Dec. 12, 2002, <http://www.extremetech.com/article2/0,1697,760735,00.asp>.

¹¹⁵ For example, over 700 of the individuals whose personal information was released in the ChoicePoint data spill reported that they had been the victim of identity theft. SOLOVE ET AL., *supra* note 10, at 699.

¹¹⁶ *Id.* at 696.

¹¹⁷ IDENTITY THEFT RESOURCE CENTER, IDENTITY THEFT: THE AFTERMATH 2004, at 2 (2005), available at <http://www.idtheftcenter.org/aftermath2004.pdf> (posting national survey of identity theft victims).

rating.¹¹⁸ Almost ten million Americans suffered identity theft in 2003, resulting in losses of 300 million hours and \$5 billion.¹¹⁹

A fictional example illustrates the potential threat to informational privacy in the digital age. Donna¹²⁰ has worked for some years for the state government. A year ago, Donna was diagnosed with adult-onset diabetes. Donna's body fails to produce sufficient amounts of insulin, and as a result, glucose has been building up in Donna's blood.¹²¹ If left untreated, this condition can increase the risk of heart disease and stroke, kidney failure, retinal damage and blindness, and nerve damage.¹²² Donna has not yet experienced these serious complications but, due to the early symptoms, had to take several consecutive weeks of sick leave. During that time, Donna met with her physician to discuss a treatment plan and also conducted her own research on how best to manage the disease. She resolved to reduce the amount of sugars in her diet.¹²³ To that end, she decided to purchase sugar-free foods wherever possible. Recently, Donna decided to leave her current position and pursue her dream of working for an airline. She applied to the major airlines for a job working behind the ticket counter.

In an analog world, Donna's activities would have generated few records: a card with her signature when she went to the library and signed out books about diabetes, paper receipts reflecting her purchase of sugar-free foods, and personnel records keeping track of her sick leave. All of these records would have been stored in file

¹¹⁸ R. Bradley McMahon, Note, *After Billions Spent to Comply with HIPAA and GLBA Privacy Provisions, Why Is Identity Theft the Most Prevalent Crime in America?*, 49 VILL. L. REV. 625, 626 (2004).

¹¹⁹ SOLOVE ET AL., *supra* note 10, at 696 (citing FTC, IDENTITY THEFT SURVEY REPORT 4, 6 (Sept. 2003), available at <http://www.ftc.gov/os/2003/09/synovatereport.pdf>).

¹²⁰ All of the individuals and entities described in this hypothetical are intended to be purely fictional.

¹²¹ For information about adult-onset diabetes, also known as Type 2 Diabetes, see Am. Diabetes Ass'n, Type 2 Diabetes, <http://www.diabetes.org/type-2-diabetes.jsp> (last visited Sept. 17, 2006).

¹²² Am. Diabetes Ass'n, Type 2 Diabetes Complications, <http://www.diabetes.org/type-2-diabetes/complications.jsp> (last visited Sept. 17, 2006).

¹²³ For information on the importance of reducing sugar intake, see Am. Diabetes Ass'n, Frequently Asked Questions About Nutrition, available at <http://www.diabetes.org/nutrition-and-recipes/nutrition/faqs.jsp> (last visited Sept. 17, 2006) (explaining importance of reducing sugar intake).

cabinets such that a great deal of time and effort would have to be spent to collect and compile them.

Digitization radically changes this. Instead of filing Donna's sick leave records in an inaccessible cabinet, the state enters them into a computer database. OmniData, a data mining company, makes a public records request and obtains digitized employee data from the state, including Donna's sick leave information.¹²⁴ Instead of going to the library, Donna conducts her research at MedInform.com, a website that specializes in medical advice. She fills out a registration form on which she provides her name and email address. MedInform.com discretely places a "cookie" on her computer that it uses to track the pages she views during her various visits, including all of her research on diabetes.¹²⁵ It then puts together a computer profile of Donna, which the registration form allows it to link not only to her computer, but also to her name, and sells it to OmniData, which combines it with the other information it possesses about Donna.¹²⁶ Finally, Donna purchases her sugar-free products at the grocery store. She uses her customer loyalty card to obtain a small discount and her Mastercard to make the purchase. The store records all purchases made using loyalty cards and is able to match them with the name on the card.¹²⁷ The store, too, sells this information to OmniData.¹²⁸

¹²⁴ See Solove, *supra* note 12, at 1144 (noting state governments release individual sick leave records to public); see also *State ex. rel. Beacon Journal Publ'g Co. v. City of Akron*, 640 N.E.2d 164, 165 (Ohio 1994) (noting State of Ohio releases employee "sick leave information" in response to public records request).

¹²⁵ See Kang, *supra* note 11, at 1227 (explaining what a cookie is and does).

¹²⁶ Medical advice sites have been found to transfer information to third parties, in direct contravention of their stated privacy policies. Tynan, *supra* note 104 (discussing study that shows many health advice sites collect information through cookies and transfer it to third parties including insurers and potential employers). The HIPAA privacy rule does not cover this transfer of data because the website is only providing health information and is not providing "health care" as defined in the regulation. See ANGELA CHOY ET AL., PEW INTERNET & AM. LIFE PROJECT, EXPOSED ONLINE: WHY THE NEW FEDERAL HEALTH PRIVACY REGULATION DOESN'T OFFER MUCH PROTECTION TO INTERNET USERS 11-13 (2001), available at http://www.pewinternet.org/pdfs/PIP_HPP_HealthPriv_report.pdf (explaining HIPAA terms).

¹²⁷ Elect. Privacy Info. Ctr., *Privacy and Consumer Profiling*, <http://www.epic.org/privacy/profiling/> (last visited Aug. 30, 2006) (noting supermarkets use club cards to create detailed profiles of individual consumption habits and link to individually identifiable information).

¹²⁸ *Id.* (noting supermarkets sell this information to data aggregators).

OmniData puts all of this data together in order to infer additional, latent information.¹²⁹ It can now see that Donna did not purchase sugar-free products solely to lose weight. By viewing this purchase in association with her sick leave, and medical treatment inquiries it can infer a strong probability that she has diabetes and is taking steps to treat this illness.¹³⁰ All of the major airlines have contracted with OmniData to screen their job applicants.¹³¹ OmniData flags Donna's application as one that poses a risk of serious health issues.¹³² In an effort to control health insurance costs, each airline denies Donna an interview.¹³³ To make matters worse, the credit card processor that handled Donna's Mastercard transaction experiences a major data spill.¹³⁴ Computer hackers

¹²⁹ Fulda, *supra* note 12, at 106. Data miners use "association rules" to accomplish this. Zarsky, *supra* note 15, at 12. Such rules use

algorithms in searching the database to reveal patterns of variables that typically associate with each other. . . . The algorithms "check" whether there are any *rules* that could describe the relation between various variables in the examined databases. These "rules" (or patterns) refer to logical statements such as: *If A = 1 and B = 1 then C = 1*

Id.

¹³⁰ See Elect. Privacy Info. Ctr., *supra* note 127 (noting that computer profilers combine individual identities with many other attributes including health information).

¹³¹ See Solove, *supra* note 12, at 1151 (noting employers purchase information from data mining companies and use it to screen new hires); cf. Joshua Quittner, *Invasion of Privacy*, TIME, Aug. 25, 1997, at 28, 31–32 ("At least a third of all Fortune 500 companies regularly review health information before making hiring decisions.").

¹³² See Elect. Privacy Info. Ctr., *supra* note 127 (describing how Medical Marketing Service sells lists of persons suffering from many ailments including diabetes).

¹³³ See Solove, *supra* note 12, at 1151 (noting employers acquire information from data brokers and use it to screen potential employees); Tynan, *supra* note 104 (describing possibility that medical advice sites sell individual health profiles to employers who can then use them "to screen out job applicants based on health advice they may have sought on the Web . . . [and] lower their insurance premiums by not hiring employees who could potentially have serious illnesses"); Zarsky, *supra* note 15, at 20 (discussing hypothetical where company purchases information about employee's heart condition and accordingly dismisses employee).

Several circuits have held that diabetes does not qualify as a disability for the purposes of the Americans with Disabilities Act (ADA), although at least one circuit has held that it does. See, e.g., *Salim v. MGM Grand Detroit, L.L.C.*, 106 F. App'x 454, 458–61 (6th Cir. 2004) (finding plaintiff with diabetes is not substantially limited in performing a major life activity under the ADA); *Nawrot v. CPC Int'l*, 277 F.3d 896, 904 (7th Cir. 2002) ("[D]iabetic status, per se, is not sufficient to qualify as a disability under the ADA."). But see *Fraser v. Goodale*, 342 F.3d 1032, 1041 (9th Cir. 2003) (finding material issue of fact as to whether diabetes limits major life activity of eating). Assuming that the airlines in our hypothetical were domiciled in one of the circuits that does not view diabetes as a disability, their decision to screen Donna out due to her diabetic condition should not violate the ADA.

¹³⁴ For an example of a true incident of this nature, see *Dash & Zeller*, *supra* note 113

steal Donna's name, credit card number, and security code. An identity thief runs up \$10,000 in purchases on her credit card. Donna has to spend much time and money sorting out this mess and is never able to re-establish her good credit rating. The Information Revolution has indeed damaged Donna's privacy.

III. PRIVACY INJURIES ARE LIKE ENVIRONMENTAL HARMS

The privacy injuries of the Information Age are structurally similar to the environmental damage of the smokestack era. Two key concepts that have been used to understand environmental damage—the “negative externality” and the “tragedy of the commons”—also shed light on privacy injuries.

A. NEGATIVE EXTERNALITIES

Negative externalities exist whenever someone utilizes a resource but is able to impose on others the costs of that use.¹³⁵ The costs are said to be “external” to the user and to result in “negative externalities.”¹³⁶ For example, a manufacturer of steel pipes must pay to use resources such as iron or labor. If it wishes to emit pollutants, however, the costs (such as respiratory problems among the surrounding populace) are borne not by the manufacturer but by others in society. Since it does not have to bear these costs, the company has little incentive to minimize them. Instead, it will wastefully “use up” the clean air resource in the way that it would never consume iron, labor, or any other resource for which it had to pay.¹³⁷ This leads the company, and others like it, to create too much air pollution and other negative externalities. To solve this problem, it is necessary to force the company to bear or “internalize” the costs of the pollution that it is creating. Only then will it have an incentive to reduce it.¹³⁸

(describing data spill by credit card processor that may have led to identity theft).

¹³⁵ See SALZMAN & THOMPSON, *supra* note 30, at 17–18 (noting externality exists where factory pollutes air but does not have to pay costs associated with this pollution).

¹³⁶ *Id.* at 18.

¹³⁷ *Id.*

¹³⁸ *Id.* (“[Where] factory has to pay for the external harm it causes, then it will reduce its pollution. The process for forcing the factory to recognize environmental and social costs is

B. THE TRAGEDY OF THE COMMONS

The “tragedy of the commons” explains how economically rational, self-interested use of a commonly owned resource can result in the destruction of that resource.¹³⁹ The classic example, drawn from an essay by Garrett Hardin, concerns cattle herders who graze their animals on a commonly owned field of grass.¹⁴⁰ Hardin theorized that from the perspective of the individual cattle herder it is rational to increase the number of his cattle that are grazing in the field. He gets the full benefit of adding another animal but shares the cost of using up the grass with all others who have the right to graze in the field.¹⁴¹ The individual herder, pursuing his self-interest, will accordingly add another head of cattle to the field, then another, and so on. So will the other herders. Eventually, there will be so many cattle that they will eat down the grass to the point that it cannot regenerate itself, rendering the field useless for grazing purposes. All cattle herders will lose access to the resource. What was individually rational turns out to be collectively ruinous.¹⁴² The same dynamic can be seen when fishermen exploit ocean stocks to the point that the fish population crashes or when farmers draw water from a common aquifer at such a rate that it is not able to recharge itself and stops producing plentiful water.¹⁴³ In each of these situations, the users’ over-exploitation of the resource ends up depriving them of its benefits. It is this characteristic that separates a “true” tragedy of the commons from other situations in which exploiters of common resource impose externalities but do not diminish their own ability to utilize the resource.¹⁴⁴

known as *internalizing the externalities*.”).

¹³⁹ The tragedy of the commons thus serves as a counterpoint to Adam Smith’s “invisible hand” which posits that the pursuit of individual self-interest will enhance the wealth of the larger society. See Shi-Ling Hsu, *What Is a Tragedy of the Commons? Overfishing and the Campaign Spending Problem*, 69 ALB. L. REV. 75, 78–79 (2005) (contrasting Hardin and Smith).

¹⁴⁰ See generally Garrett Hardin, *The Tragedy of the Commons*, 162 SCIENCE 1243 (1968) (discussing phenomenon known as “tragedy of the commons”).

¹⁴¹ *Id.* at 1244.

¹⁴² See *id.* (“Freedom in a commons brings ruin to all.”); see also SALZMAN & THOMPSON, *supra* note 30, at 16 (“[I]ndividually rational behavior is collectively deficient.”).

¹⁴³ SALZMAN & THOMPSON, *supra* note 30, at 16–17.

¹⁴⁴ See Hsu, *supra* note 139, at 76 (“[A] true tragedy of the commons specifically involves

C. SPAM, EXTERNALITIES, AND THE TRAGEDY OF THE COMMONS

These concepts provide insight into the spam problem. A spammer incurs small costs for computer equipment and labor¹⁴⁵ but imposes the larger costs of his activity—the time spent deleting spam, the cost of filters, the lost email messages, and the higher connection fees—on the recipients of his email barrage.¹⁴⁶ Spam spewed from a computer thus creates a negative externality in much the same way that air emissions from a smokestack do.¹⁴⁷ Since spammers have no incentive to limit these external costs, they wastefully use up the “inbox” resource sending as many as 250 million spam emails *per day*.¹⁴⁸ As in the environmental context, the way to get spammers to reduce this flow is to force them to internalize the costs of their spam.

The failure to do so may well lead to a classic tragedy of the commons.¹⁴⁹ To understand this, it is important to view the situation from the spammer’s perspective. Any spammer in possession of the proper email address may use it to market a

a situation in which the resource users are detracting from their own ability to continue to exploit the resource.”).

¹⁴⁵ The cost to a spammer of sending an email message is roughly 0.019 cents per message. MARTIN ABADI ET AL., *BANKABLE POSTAGE FOR NETWORK SERVICES 2* (Springer-Verlag 2003) (copy on file with author), available at <http://research.microsoft.com/research/sv/pennyblack/demo/ticketserver.pdf>.

¹⁴⁶ See Zhang, *supra* note 87, at 305 (“Unlike traditional methods of advertising, spam imposes the bulk of advertising fees on recipients rather than spammers.”); see also *supra* notes 88–94 and accompanying text (describing these costs).

¹⁴⁷ See Mossoff, *supra* note 27, at 665 (“In economists’ terms, spammers are *creating negative externalities* through the use of their email accounts.”) (emphasis added); see also Hirsch, *supra* note 28, at 244. In at least one respect, spam may appear to differ from environmental pollution. In the environmental context, the polluter intends to make a useful product and pollutes as an incidental side-effect of this activity. In the spam situation, the spammer intends to send the email, and the harm arises directly from this. But are the situations really so different? A spammer’s intent is to market a product, not to clog up an inbox. In fact, most spammers will not want to overcrowd an inbox since this will be detrimental to spam marketing. Much like a polluter, the spammer intends to produce something useful from his viewpoint (an advertisement) but ends up damaging others as an inherent side-effect of this behavior. It may be more difficult to distinguish the beneficial from the harmful side of the spammer’s activity because both are contained within the same email message. But that does not change the fact that, as in the environmental arena, the spammer’s activity has both a positive and a negative component, and the harmful side is externalized onto others.

¹⁴⁸ See *supra* note 85 and accompanying text.

¹⁴⁹ Hirsch, *supra* note 28, at 244–45.

product,¹⁵⁰ and so all may be said to have access to this resource. From the spammer's perspective, the benefit to sending an additional email lies in the increased chance of making a sale. The cost lies in using up the attention that the recipient can devote to reading email, thus decreasing the chance that the recipient will actually view any given marketing message. As with Hardin's cattle herder, the spammer appropriates the full benefit of each email (in terms of the opportunity to make a sale) but shares the cost (in terms of the recipient's reduced attention) with all other spammers who are trying to market to that recipient. Moreover, the spammer knows that if he refrains from sending an email in order to reduce the recipient's email burden, his competitors are likely to fill the space he has left free.¹⁵¹ These circumstances, coupled with the minimal cost of sending additional email,¹⁵² will cause the rational spammer to send out more and more email just as they convince cattle herders to continue to add more and more cattle. This explains the alarming trend in the number of spam emails over the past few years—140 billion spam messages in 2001,¹⁵³ 261 billion in 2002,¹⁵⁴ and 2 trillion in 2004¹⁵⁵—with no end in sight. Spammers have become like cattle herders, driving more and more of their beasts into the commons to gobble up the available grass, although here the cattle are spam messages, the commons is the available space in the inbox (or conceptualized differently, the available

¹⁵⁰ See Hsu, *supra* note 139, at 79 n.25 (defining "open access" resource). Filtering devices can edit out some spam messages and thus limit access to the inbox commons. But the emergence of these programs has led to little more than a technological arms race with the spammers, who are continually coming up with ways to circumvent the filters. Mossoff, *supra* note 27, at 630. Moreover, if the filters become too fine, then desired emails might be diverted or deleted, thereby destroying the utility of email—another tragedy, but this one achieved by means of excessive fencing rather than excessive use.

¹⁵¹ See Hsu, *supra* note 139, at 94 (noting that in true tragedy of the commons, users of resource are generally rivals in their race to exploit it).

¹⁵² As noted above, the cost is 0.019 cents per message. ABADI ET AL., *supra* note 145, at 2; see also Robert E. Kraut et al., *Pricing Electronic Mail to Solve the Problem of Spam 4* (Yale Int'l Ctr. for Fin., Working Paper No. 05-24, 2005) (copy on file with author), available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=753664 (arguing that low cost of sending email makes it "economically rational for individual commercial emailers to distribute their messages as widely as possible").

¹⁵³ See *supra* note 86 and accompanying text.

¹⁵⁴ Mossoff, *supra* note 27, at 627.

¹⁵⁵ Zhang, *supra* note 87, at 304; see also *supra* note 87 and accompanying text.

attention of the recipient), and the grass is the lucrative business of selling Viagra, mortgages, or pornography.

As with the grazing field, the logical result of this behavior will be to ruin the inbox as a valuable marketing resource. Individuals will receive so many spam messages that they will begin to ignore all of them, filter them all out, or abandon email for other modes of communication and shut down their inboxes (under our analogy, this would be equivalent to the destruction of the grazing field). Congress has recognized this very risk, stating that “[l]eft unchecked at its present rate of increase, spam may soon undermine the usefulness and efficiency of e-mail as a communications tool.”¹⁵⁶ It may turn people off from using email, thereby destroying the very resource that spammers relied on in the first place.¹⁵⁷ This makes the spam phenomenon a true tragedy of the commons since those exploiting the inbox (the spammers) will have damaged their own ability to make use of this resource for their marketing campaigns (in addition to causing a lot of harm to individual email users along

¹⁵⁶ S. REP. NO. 108-102, at 6, as reprinted in 2004 U.S.C.C.A.N. 2348, 2352; see also Hansell, *supra* note 90 (noting that Internet service providers believe email is becoming “an increasingly unreliable” mode of communication); Kraut et al., *supra* note 152, at 3 (stating that spam is “growing rapidly and threatens to choke off e-mail as a reliable and efficient means of communication over the Internet”).

¹⁵⁷ See “*Unsolicited Commercial Email*” Before the U.S. Senate Committee on Commerce, Science and Transportation, 108th Cong. (2003), available at 2003 WL 21187271 (statement of Mozelle W. Thompson, Commissioner, Federal Trade Commission) (“[T]he volume of unsolicited email is increasing exponentially and . . . we are at a ‘tipping point,’ requiring some action to avert deep erosion of public confidence in email that could hinder, or even destroy, it as a tool for communication and online commerce.”) (emphasis added); Dennis O’Reilly, *Is E-Mail Doomed?*, PC WORLD, June 21, 2004, <http://www.pcworld.com/article/id/116606/article.html> (stating that some experts worry “it won’t be possible to sufficiently stem the tide” as people are moving away from email); see also CAN-SPAM Act of 2003, 15 U.S.C.A. § 7701(a)(2) (West 2003) (finding that “[t]he convenience and efficiency of electronic mail are threatened by the extremely rapid growth in the volume of unsolicited commercial electronic mail”); S. REP. NO. 108-102, at 7 (“[I]ndustry analysts are concerned that this trend could influence millions of consumers to abandon the use of e-mail messaging as a viable means of communication.”).

the way).¹⁵⁸ Left unchecked, spam will result in the killing of “the killer ap.”¹⁵⁹

D. PERSONAL INFORMATION, EXTERNALITIES, AND THE TRAGEDY OF THE COMMONS

When a website gathers and sells personal information about one of its users, or an Internet marketer or data miner uses this information, they cause that individual to lose a degree of privacy. This cost is borne by the user and is external to the business. It is a negative externality.¹⁶⁰ As in the environmental context, this means that the companies involved have little incentive to curtail their use and so will tend to over-engage in the activities that create the externalities.¹⁶¹ “In economic terms, the companies collecting personal information impose a negative externality on consumers. Because these companies benefit from the information they collect, but do not face the costs they impose (i.e., the violation of consumers’ privacy), they collect ‘too much’ information.”¹⁶² Just as factories have no reason to refrain from filling the air with pollutants, these

¹⁵⁸ When excessive spam causes an individual to abandon email, this harms more than the spammers. It also injures the individual associated with that email account (the recipient) and those who send nonspam messages to that person. Yet these additional injuries do not change the core fact that the spammers, through their over-exploitation of the inbox resource, are also damaging themselves. It is this that makes the spam situation a true tragedy of the commons. Hsu, *supra* note 139, at 76, 80–82. Were they to recognize the long-term implications of the situation and have a means of reaching a rough consensus, such users might well invite regulation in order to avoid the destruction of their common resource. *Id.* at 80.

¹⁵⁹ See O’Reilly, *supra* note 157. The process is already underway. According to a 2003 poll by Pew Internet and American Life Project, 25% of respondents said that spam is already causing them to curtail their use of email. Jonathan Krim, *Senate Votes 97–0 to Restrict E-Mail Ads: Bill Could Lead to No-Spam Registry*, WASH. POST, Oct. 23, 2003, at A01.

¹⁶⁰ See Hirsch, *supra* note 28, at 245.

¹⁶¹ See Schwartz, *supra* note 37, at 833 (noting that users of personal data are likely to engage in “wasteful behavior” because they do not have to pay true costs of using it).

¹⁶² Hahn & Layne-Farrar, *supra* note 66, at 16; see also PETER P. SWIRE & ROBERT E. LITAN, NONE OF YOUR BUSINESS: WORLD DATA FLOWS, ELECTRONIC COMMERCE, AND THE EUROPEAN PRIVACY DIRECTIVE 8 (Brookings Inst. Press 1998) (noting companies “internalize[] the gains from using the information but can externalize some of the losses and so ha[ve] a systematic incentive to overuse it”); Nehf, *supra* note 28, at 79–80 (noting misuse of personal information, like environmental damage, “imposes significant external costs”); Samuelson, *supra* note 11, at 1132–33 (“[F]irms collect and process personal data . . . [b]ecause they are not forced to internalize the societal costs of private sector processing of personal data.”).

companies will not hesitate to collect, use, and flood the market with detailed, personal information.¹⁶³

Once again, a tragedy of the commons lurks around the corner.¹⁶⁴ Here, the “commons” is the collective willingness of individuals to reveal their personal information on the Web. It is the trust that their informational privacy will, more or less, be respected. Each time a website sells personal data, a data miner infers sensitive information, or a data spill exposes people to identity theft, a bit of that trust is lost, and a bit of the commons disappears. Websites, marketers, and data miners receive all the benefits of their use of personal information but share the cost (in terms of the erosion of trust) with all others who depend on individuals to provide personal information on the Web. This gives them an incentive to continue collecting, selling, and using as much personal information as they possibly can.¹⁶⁵ Companies that refrain from doing so will generally lose out to competitors who are not so temperate.¹⁶⁶ This increases the incentive to make use of the information while the individual is still willing to share it. The end result promises to eat up and destroy the very willingness to reveal personal data that these businesses depend on. As with spam, this will be a true tragedy of the commons because over exploitation of the personal information resource will end up harming those who are engaged in the exploitation.¹⁶⁷ Studies show that this is already happening. According to one poll, “an overwhelming majority of Americans consistently report that they are deterred from using the Internet more than they currently do because of privacy-related fears.”¹⁶⁸

¹⁶³ Of course, the factory harms the external environment, while the privacy loss is an internal one. If the phrase is not too glib, such privacy harms could accordingly be referred to as “*internal externalities*.” I am indebted to Professor Craig Nard for helping me coin this (hopefully) amusing phrase.

¹⁶⁴ Hirsch, *supra* note 28, at 245–46.

¹⁶⁵ See TURKINGTON & ALLEN, *supra* note 3, at 420 (“Disclosure of personal data is costless to firms and may net profits, creating incentives to overuse such data.”).

¹⁶⁶ The exception would be the company that is able to “brand” itself as being especially protective of consumer privacy and turn this into a competitive advantage.

¹⁶⁷ Hsu, *supra* note 139, at 76 (defining a “true” tragedy of the commons).

¹⁶⁸ Litan, *supra* note 3, at 1058 & n.46 (citing Harris survey finding that “92% of consumers are ‘concerned’ and 67% are ‘very concerned’ about misuse of their personal data online”). Others recount that “an installed base of millions of users can quickly evaporate if customers do not trust the provider” to treat their personal information with care. Samuelson, *supra* note 11, at 1160.

Carried to its logical conclusion, this trend will lead consumers to abandon e-commerce and other online activities for “real” equivalents that protect privacy better.¹⁶⁹ Consumer trust—the commons on which the data driven businesses rely—will erode. This will undermine the viability of e-commerce and other beneficial online activities.

IV. ENVIRONMENTAL LAW AND POLICY AS A MODEL FOR PRIVACY REGULATION

How can we avoid the tragedy of the commons that threatens email, e-commerce, and other online activity? Here, too, there is much to learn from environmental law and policy. The field has spent forty years preventing just such tragedies in the natural world. Many programs have been implemented, regulatory experiments conducted, reports written, and policy discussions held. This abundance of activity has made environmental law and policy—perhaps more than any other area of administrative practice—the center of creative thinking about regulation.¹⁷⁰

This experience could greatly benefit the privacy field. Today, there is a growing sense that the Information Revolution has produced unprecedented damage to privacy. There have been numerous calls for legislation and regulation,¹⁷¹ and some has been enacted.¹⁷² Yet even as the desire for government intervention has

¹⁶⁹ Samuelson, *supra* note 11, at 1129 (“The trust necessary for electronic commerce to flourish requires the interests of individuals in information privacy to be given appropriate deference. . . .”); accord Netanel, *supra* note 79, at 474 (“[C]onsumers will not use the Internet for electronic commerce unless they are assured about personal privacy protection.”).

¹⁷⁰ SALZMAN & THOMPSON, *supra* note 30, at 41.

¹⁷¹ See Hahn & Layne-Farrar, *supra* note 66, at 29–50 (surveying recent and proposed privacy legislation).

¹⁷² See, e.g., Gramm-Leach-Bliley Financial Modernization Act of 1999, Pub. L. No. 106-102, 113 Stat. 1338 (codified in scattered sections of 12, 15, 16 & 18 U.S.C.) (protecting financial data); Children’s Online Privacy Protection Act of 1998, Pub. L. No. 105-277, 112 Stat. 2681 (codified at 15 U.S.C. §§ 6501–6506 (2000)) (protecting children under thirteen from online collection of personal information); Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended at 18 U.S.C. §§ 2510–2520, 2701–2711, 3121–3127 (2000)) (protecting against monitoring of electronic communications such as telephone calls or emails); Identity Theft and Assumption Deterrence Act of 1998, Pub. L. No. 105-318, 112 Stat. 3007 (codified as amended at 18 U.S.C. § 1028(a)(7), (b)(1), 28 U.S.C. § 994 (2000)) (making identity theft a crime); Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (codified as amended in scattered sections of

grown, it has been countered by those who argue that it will undermine personal freedom in the online world and will hurt the competitiveness of emerging, information-based businesses.¹⁷³ As one commentator has noted, the “dominant rhetoric” today espouses the view that “[t]he market, bottom-up, and industry self-regulation are to be the essential elements of any solution . . . [because] the right answer is never the State, top-down, or the law.”¹⁷⁴ The privacy debate thus centers on a tension between the desire to protect important societal values (privacy), and concerns about the regulatory burdens on individuals and firms.

These are exactly the issues that environmental law and policy have been wrestling with for decades. The federal environmental statutes of the 1970s—the “first generation” of environmental law—employed a top-down regulatory model in which government pushed emitters to adopt specific pollution control technologies.¹⁷⁵ There followed a growing debate over this “command-and-control” strategy.¹⁷⁶ Out of this discussion has flowed a more contemporary

26, 29, and 42 U.S.C.) (protecting health records).

¹⁷³ See, e.g., Jay P. Kesan & Andres A. Gallo, *Optimizing Regulation of Electronic Commerce*, 72 U. CIN. L. REV. 1497, 1498 (2004) (discussing those who prize Internet because it is government-free zone); Litan, *supra* note 3, at 1055–56 (describing ideal of Net as “example of unplanned, private sector innovation, the benefits of which could be curtailed, perhaps dramatically, by premature and ill-advised government intervention”); *Internet Regulation: Will It Hinder or Help Small Business*, BUS. WK., May 6, 1999, <http://www.businessweek.com/smallbiz/news/date/9905/f990506.htm> (quoting expert as saying “regulation will heap costs on Net businesses . . . and hinder the creative uses of information that have made the fledgling E-commerce world so vibrant”).

¹⁷⁴ Schwartz, *supra* note 37, at 848 (identifying this view and critiquing it); *accord* TURKINGTON & ALLEN, *supra* note 3, at 428 (stating that polls show public does not want regulation to constrain information economy); Kesan, *supra* note 37, at 94 (noting that debate over top-down versus bottom-up regulation has led both government and private industry to “prefer self-regulation”); Litan, *supra* note 3, at 1045 (stating that in regulating Internet, “policymakers’ first instinct should be to rely on markets and technology to address troublesome issues”).

¹⁷⁵ See Hirsch, *supra* note 30, at 1–2 (describing “first generation” environmental regulation).

¹⁷⁶ For critiques of command-and-control regulation as it has been applied in the environmental field, see generally BRUCE A. ACKERMAN & WILLIAM T. HASSLER, *CLEAN COAL/DIRTY AIR: OR HOW THE CLEAN AIR ACT BECAME A MULTIBILLION-DOLLAR BAIL-OUT FOR HIGH-SULFUR COAL PRODUCERS AND WHAT SHOULD BE DONE ABOUT IT* (Yale Univ. Press 1981); IAN AYRES & JOHN BRAITHWAITE, *RESPONSIVE REGULATION: TRANSCENDING THE DEREGULATION DEBATE* (Oxford Univ. Press 1992); J. CLARENCE DAVIES & JAN MAZUREK, *POLLUTION CONTROL IN THE UNITED STATES: EVALUATING THE SYSTEM* (1998); *THINKING ECOLOGICALLY: THE NEXT GENERATION OF ENVIRONMENTAL POLICY* (Marian R. Chertow & Daniel C. Esty eds., Yale Univ.

set of regulatory instruments—often referred to as the “second generation” of environmental regulation—that seeks to be more flexible and cost-effective while still providing strong environmental protection.¹⁷⁷ This experience should prove useful to the emerging area of privacy regulation. Briefly stated, the environmental experience suggests that top-down regulation, while the right choice for addressing some social ills, is not the best method for regulating the highly dynamic and competitive digital economy.¹⁷⁸ By contrast, second generation regulatory approaches appear well suited to this area.¹⁷⁹ Indeed, as later parts of this Article will describe, some in the privacy field are already taking steps that resemble second generation strategies, although they appear to be doing so without a complete understanding of the regulatory methods that they are emulating.¹⁸⁰ The remainder of this Part will explain why governance of the digital economy would be better served by second generation rather than first generation regulatory strategies. The following Parts will then describe the most relevant second generation methods in some detail and explain how they could be productively adapted for protecting privacy in the Information Age.

A. COMMAND-AND-CONTROL REGULATION WOULD NOT BE A GOOD FIT FOR THE DIGITAL ECONOMY

Press 1997) [hereinafter THINKING ECOLOGICALLY] (analyzing second generation strategies); Bruce A. Ackerman & Richard B. Stewart, *Reforming Environmental Law*, 37 STAN. L. REV. 1333 (1985); Eric W. Orts, *Reflexive Environmental Law*, 89 NW. U. L. REV. 1227 (1995). For defenses of the traditional system, see generally Howard Latin, *Ideal Versus Real Regulatory Efficiency: Implementation of Uniform Standards and “Fine-Tuning” Regulatory Reforms*, 37 STAN. L. REV. 1267 (1985); Sidney A. Shapiro & Thomas O. McGarity, *Not So Paradoxical: The Rationale for Technology-Based Regulation*, 1991 DUKE L.J. 729 (1991); Rena I. Steinzor, *Reinventing Environmental Regulation: The Dangerous Journey from Command to Self-Control*, 22 HARV. ENVTL. L. REV. 103 (1998). For a summary of the debate with citations to many of the leading sources, see Stewart, *supra* note 29, at 21–24 & n.1.

¹⁷⁷ See THINKING ECOLOGICALLY, *supra* note 176 (analyzing second generation strategies); Hirsch, *supra* note 30, at 5–15 (describing second generation initiatives); J.B. Ruhl, *Endangered Species Act Innovations in the Post-Babbitonian Era—Are There Any?*, 14 DUKE ENVTL. L. & POL'Y F. 419, 428–30 (2004) (describing regulatory innovation in area of natural resources law and policy). See generally Stewart, *supra* note 29, at 38–151 (providing comprehensive analysis of second generation strategies).

¹⁷⁸ See *infra* notes 181–205 and accompanying text.

¹⁷⁹ See *infra* notes 207–22 and accompanying text.

¹⁸⁰ See *infra* notes 283–327 and accompanying text.

The environmental experience suggests that those who oppose regulation of the digital economy are largely correct in contending that traditional command-and-control laws should not be employed. As developed in the first generation of federal environmental laws,¹⁸¹ the command-and-control method begins with government officials designating the industry that must curtail its emissions.¹⁸² Next, regulators identify the best currently existing technology for controlling pollution in that industry (known as the “reference technology”).¹⁸³ Finally, government officials either direct all facilities in the industry to install the chosen technology (this is known as a “design standard”)¹⁸⁴ or require that they not exceed the *rate of pollution* that they would emit if they had installed the reference technology (this is known as a “rate-based standard”).¹⁸⁵ In theory, rate-based standards allow facilities to come up with their

¹⁸¹ All of these statutes rely heavily on command-and-control. U.S. CONGRESS, OFFICE OF TECH. ASSESSMENT, ENVIRONMENTAL POLICY TOOLS: A USER'S GUIDE 2 (1995) [hereinafter ENVIRONMENTAL POLICY TOOLS]; Hirsch, *supra* note 30, at 1–2.

¹⁸² Ackerman & Stewart, *supra* note 176, at 1335 (summarizing Best Available Technology (BAT) regulatory strategy); Hirsch, *supra* note 30, at 1–2 (same).

¹⁸³ Ackerman & Stewart, *supra* note 176, at 1335; Hirsch, *supra* note 30, at 1–2; *see also* ROBERT V. PERCIVAL ET AL., ENVIRONMENTAL REGULATION: LAW, SCIENCE, AND POLICY 128 (Aspen Publishers, 4th ed. 2003) (explaining technology specifications). Identifying such technology often requires regulators to visit facilities, review the design and engineering specifications of current control technologies, and evaluate whether they are feasible for the industry as a whole. Ackerman & Stewart, *supra* note 176, at 1336–37.

¹⁸⁴ PERCIVAL ET AL., *supra* note 183, at 128. An example would be Resource Conservation and Recovery Act (RCRA) standards that require that, on pain of penalties, all new hazardous waste landfills install two more liners to prevent leaching of hazardous material into the ground. Solid Waste Disposal Act, 42 U.S.C. § 6924(o)(1)(A)(i) (2000).

¹⁸⁵ *See* Byron Swift, *How Environmental Laws Work: An Analysis of the Utility Sector's Response to Regulation of Nitrogen Oxides and Sulfur Dioxide Under the Clean Air Act*, 14 TUL. ENVTL. L.J. 309, 407 (2001) (describing rate-based approach). For example, the Clean Air Act New Source Performance Standards for the industry that coats beverage cans require that new facilities emit no more than 0.29 kg of volatile organic compounds (an air pollutant usually referred to as “VOC”) per liter of coating liquid used. Standards of Performance for the Beverage Can Surface Coating Industry, 40 C.F.R. § 60.492(a) (2004). This rate-based standard reflects the amount that these plants would emit if they used waterborne coatings—the “reference” technology chosen by the agency. Standards of Performance for New Stationary Sources; Beverage Can Surface Coating Industry, 48 Fed. Reg. 38,728, 38,728 (Aug. 25, 1983). In theory, a rate-based standard should allow facilities to choose their own means of achieving the required emission rate. For example, a beverage can coating facility could choose to use solvent-borne coatings, which emit more VOC, in combination with an emission control system that would capture the increased VOC. *Id.* However, if it did so, it would have to go to great lengths to prove to the agency that its unique method actually achieved the same results as the waterborne coatings that the agency had recommended.

own control method. In practice, almost all choose the reference technology so as to avoid any misunderstandings about compliance.¹⁸⁶ Command-and-control regulation thus either requires, or strongly pushes, firms to adopt the control technology that the government has chosen for them.¹⁸⁷

This approach has the advantage of being easy to monitor and enforce.¹⁸⁸ If assurance of pollution reduction is the top priority—as it is, for example, when toxic emissions are being released into the environment—then command-and-control might well be the method of choice.¹⁸⁹ Yet, the environmental experience shows that the method also possesses some significant weaknesses.¹⁹⁰ To begin with, it is expensive. It requires all facilities in a given category to achieve the same emissions rate, even where the cost of pollution control varies significantly from plant to plant.¹⁹¹ A system under which those who could reduce pollution at the least cost made the bulk of the reductions would save “tens of billions” of dollars annually.¹⁹² Command-and-control also deters innovation in

¹⁸⁶ PERCIVAL ET AL., *supra* note 183, at 131; Hirsch, *supra* note 30, at 2; *see also* ENVIRONMENTAL POLICY TOOLS, *supra* note 181, at 9 (providing catalog of tools).

¹⁸⁷ ENVIRONMENTAL POLICY TOOLS, *supra* note 181, at 9 (defining “command-and-control” regulation).

¹⁸⁸ SALZMAN & THOMPSON, *supra* note 30, at 49. In most cases, the inspector’s task is simply to determine whether the reference technology is in place and whether it is operational. *Id.* Other strengths include claims that command-and-control regulation is fair because all facilities in a given industry must meet the same emissions rate standard, and that it lends itself to public participation because stakeholder groups can focus their energies on a single, national rulemaking in which the EPA sets the emissions standard for the given industry. *See* Latin, *supra* note 176, at 1271 (noting advantages of uniform standards including “greater consistency and predictability of results, [and] greater accessibility of decisions to public scrutiny and participation”); *see also* Shapiro & McGarity, *supra* note 176, at 729 (arguing BAT regulation “is rational, and stands up well when compared to the reliance on market-related regulation”).

¹⁸⁹ ENVIRONMENTAL POLICY TOOLS, *supra* note 181, at 26 (stating technology specifications are effective method for assuring that environmental goals will be met); *see also* Neil Gunningham, *Environmental Management Systems and Community Participation: Rethinking Chemical Industry Regulation*, 16 UCLA J. ENVTL. L. & POL’Y 319, 327 (1998) (noting command-and-control regulation is reliable method for improving environmental quality because “there is adequate monitoring and enforcement,” which is particularly important where “potent and toxic substances are being released into the ambient environment”).

¹⁹⁰ *See generally* Stewart, *supra* note 29, at 27–38 (describing these shortcomings).

¹⁹¹ *Id.* at 31 (“[S]ources with high costs of pollution or waste control are held to the same requirements as those with lower costs.”).

¹⁹² *Id.* at 32; *see also* ENVIRONMENTAL POLICY TOOLS, *supra* note 181, at 36 (noting command regulation is inefficient “[w]hen costs are quite variable from source to source”);

pollution prevention and locks in the current state of pollution control technology.¹⁹³ By requiring firms to meet the best *existing* level of control technology, it gives them no incentive to exceed this level.¹⁹⁴ Finally, the method is too slow for rapidly evolving industries.¹⁹⁵ By the time government regulators have promulgated a technology standard, they may have been “lapped” by changes in the industry.¹⁹⁶

These attributes do not mesh well with the digital economy. Command regulation’s chief strength—its ability to assure results—is not as critical with respect to personal information as it is with respect to the release of toxic emissions. Assurance of results

Gunningham, *supra* note 189, at 327 (revealing that prescriptive regulation, failing to recognize differences among facilities, imposes excess costs). See generally DAVIES & MAZUREK, *supra* note 176 (discussing inefficiency of traditional regulation).

¹⁹³ SALZMAN & THOMPSON, *supra* note 30, at 46; Ackerman & Stewart, *supra* note 176, at 1336 (stating that BAT controls can discourage “development of new, environmentally superior strategies”); Stewart, *supra* note 29, at 33 (“[F]irms often lack adequate regulatory incentive to reduce discharges further.”).

¹⁹⁴ Gunningham, *supra* note 189, at 327 (stating that command-and-control regulation is “biased against technological innovation . . . and provides little ongoing incentive for continuous improvement”).

¹⁹⁵ *Id.* (explaining prescriptive regulation is not well suited to industries, such as chemical manufacturing, that undergo rapid technological change). Professor J.B. Ruhl has explained that it is not only the regulated industries that are rapidly changing; the environment too is a complex adaptive system that is constantly evolving in a nonlinear fashion. J.B. Ruhl, *Thinking of Environmental Law as a Complex Adaptive System: How to Clean Up the Environment by Making a Mess of Environmental Law*, 34 HOUSTON L. REV. 933, 942–67 (1997). Environmental law thus seeks to govern two targets—the environment and the economy—that are themselves highly mutable and unpredictable. *Id.* at 967–68. This helps to explain why command-and-control regulations, which seek to prescribe a static “fix” to environmental problems, often do not achieve their intended goals. *Id.* at 940. The industries that they are seeking to regulate, and the environment that they are trying to protect, quickly evolve around them. For Ruhl, the solution is for environmental law itself to adopt the characteristics of a complex adaptive system. *Id.* at 980. He argues for a more flexible form of regulation that emphasizes experimentation, feedback, and adaptation. *Id.* at 986–91. These themes are far more consistent with second generation strategies than with the first generation, command-and-control approach.

¹⁹⁶ See Stewart, *supra* note 29, at 31 (noting that regulators are unable to gather sufficient information to write directives that meet actual facts on ground); see also ENVIRONMENTAL POLICY TOOLS, *supra* note 181, at 27–28 (recognizing that time and effort required to revise technology specifications makes it hard for traditional regulation to adapt to new technologies). The requirement that government regulators make complex engineering and design decisions can also impose huge information collection costs on regulators. Ackerman & Stewart, *supra* note 176, at 1336–37. It also provides fertile ground for adversarial advocacy by both regulated industries and environmental groups, thereby further delaying issuance of the standard and driving up costs. *Id.*

does not so easily trump regulatory cost. To the contrary, the digital economy, in which global competition is fierce and profit margins slim, highly prizes regulatory efficiency.¹⁹⁷ Command-and-control regulation, which often forgoes the most cost-effective means in favor of the most reliable one, is not the best choice.¹⁹⁸ The method's deterrence of innovation also poses a problem. Enhanced privacy protection will depend on the development of new technologies. This development will require regulatory methods that encourage innovation, not those that constrain it.¹⁹⁹ “[P]rivacy mandates—especially if they are written too prescriptively—could impede the development of even better technologies than those now available to give consumers greater power over their information without, at the same time, impeding the flow of information that now facilitates commerce.”²⁰⁰ Finally, the digital economy is driven by technological change and evolves at a far faster rate than most smokestack industries.²⁰¹ Command-and-control regulation does not function well in such fast-changing business sectors²⁰² where its technology requirements cannot keep pace with new developments. For example, assume that the government had tried to protect clickstream data by limiting the use of “cookies.” The industry would have leapfrogged “cookies” with new technologies, such as

¹⁹⁷ See George Papa Constantinou, *e-Policy: The Impact and Political Economy of the Digital Revolution*, in SOCIAL AND ECONOMIC TRANSFORMATION IN THE DIGITAL ERA 23 (Georgios Doukidis et al. eds., 2004) (discussing efficient regulation as means to encourage entrepreneurship in digital economy).

¹⁹⁸ Indeed, the chief factor that has made this method inefficient in the environmental area—the inability of uniform standards to discriminate between high- and low-cost reducers—is likely to be even more problematic in the privacy area. Digital-based industries tend to be highly heterogeneous with different business models and technologies competing against each other. It follows that the marginal costs of privacy protection are likely to vary from company to company, depending on the core technology and processes that each business employs. The lesson from environmental regulation is that nationally uniform standards, which require all regulated parties to meet the same standards, will be highly inefficient as applied to such industries.

¹⁹⁹ Litan, *supra* note 3, at 1065.

²⁰⁰ *Id.*

²⁰¹ *Id.* at 1045 (describing “fast-moving Internet environment” and challenges it poses for regulation).

²⁰² See Dennis D. Hirsch, *Lean and Green? Environmental Law and Policy and the Flexible Production Economy*, 79 IND. L.J. 611, 630–39 (2004) (explaining this weakness in reference to fast-cycle “Lean” manufacturing).

“web bugs”²⁰³ or “spyware,”²⁰⁴ that achieve the same result.²⁰⁵ The environmental experience suggests that command-and-control regulation would not be a good choice for the digital economy.²⁰⁶

B. SECOND GENERATION REGULATION WOULD WORK BETTER

In 1995, Congress’s Office of Technology Assessment issued an influential report on environmental regulatory methods.²⁰⁷ The Report concluded that “those instruments that shift responsibility for determining the means and timing of compliance to individual firms or groups of firms” are likely to generate far more cost-effective responses to environmental problems.²⁰⁸ Firms know their facilities far better than regulators and are therefore better able to come up with cost-effective pollution controls *if they set their minds to it*.²⁰⁹ As we have seen, first generation regulation actively discourages companies from undertaking this search.²¹⁰ Second generation policies are those that *encourage* facilities to come up with their own cost-effective approaches to achieving environmental goals and that allow these self-directed actions to count towards regulatory

²⁰³ See Litan, *supra* note 3, at 1058 n.45 (citing Robert O’Harrow, Jr., *Fearing a Plague of “Web Bugs”: Invisible Fact-Gathering Code Raises Privacy Concerns*, WASH. POST, Nov. 13, 1999, at E1) (defining “web bug”).

²⁰⁴ Spyware is malicious software that takes control of a user’s computer for the benefit of a third party and can be used to surreptitiously monitor the user’s online activity. Wikipedia, Spyware, <http://en.wikipedia.org/wiki/Spyware> (last visited Aug. 25, 2006).

²⁰⁵ If regulators responded by prohibiting all alternatives to the chosen technology, that would freeze technological development—another undesirable result.

²⁰⁶ This is not to say that all regulatory requirements are alike when it comes to adaptability. This Part has been focused on the highly specific, complex command-and-control regulations that are typical of environmental law. However, it is possible to develop broad, simple mandates that can be applied to many new situations. Such requirements will do a better job of keeping pace with new technologies than will the more intricate schemes found in environmental law. Cf. Daniel Solove, *Reconstructing Electronic Surveillance Law*, 72 GEO. WASH. L. REV. 1701, 1740–44 (2004) (arguing for sweeping warrant requirement that would apply to many different types of electronic surveillance utilizing wide variety of technologies).

²⁰⁷ See generally ENVIRONMENTAL POLICY TOOLS, *supra* note 181.

²⁰⁸ *Id.* at 24.

²⁰⁹ Cf. James Salzman, *Creating Markets for Ecosystem Services: Notes from the Field*, 80 N.Y.U. L. REV. 870, 887–88 (noting that prescriptive regulation does not sufficiently elicit information from landowners about best way to protect species on their property; arguing that more flexible regulatory tools would achieve this more effectively).

²¹⁰ See *supra* note 193 and accompanying text.

compliance.²¹¹ Some go even further and allow groups of companies to identify the lowest cost reducers among them and have those entities make the majority of the reductions.²¹² Such strategies are far more cost-effective than command-and-control requirements.²¹³ Second generation strategies also tend to do a better job of promoting new and better approaches to pollution reduction.²¹⁴ They move away from the single government-chosen technology standard and instead encourage facilities to come up with their own ways to improve their environmental performance. This shift promotes innovation instead of freezing the state of the art at the level of the current “best” technology²¹⁵ and can yield more effective methods that produce environmental gains. Finally, second generation initiatives encourage firms to select the control technology and thereby avoid the delays associated with government

²¹¹ The “second generation” label has been applied to a wide and diverse array of approaches. See Hirsch, *supra* note 30, at 5–15 (describing second generation initiatives); Ruhl, *supra* note 177, at 427–30 (describing regulatory innovation in area of natural resources law and policy); Stewart, *supra* note 29, at 38–151 (providing comprehensive analysis of second generation strategies). See generally THINKING ECOLOGICALLY, *supra* note 176 (analyzing array of second generation strategies). This makes it difficult to identify a single theme that unifies these initiatives. That said, most if not all of these programs give regulated parties a greater role in choosing how they will go about improving their environmental performance, and this principle can serve as a link between them.

²¹² As will be explained further below, an emission fee approach is one example. Those firms that can reduce at low cost will do so to avoid paying the fee. Those who face high reduction costs will bear the fee instead of reducing. The net result will be that the low-cost reducers make the bulk of the reductions. See *infra* notes 231–32 and accompanying text. Market-based trading strategies have the same result by allowing high-cost reducers to purchase credits and low-cost reducers to sell them. STEPHEN JOHNSON, ECONOMICS, EQUITY, AND THE ENVIRONMENT 125 (Envtl. Law Inst. 2004). Industry covenants, which allow the industry as a whole a role in deciding which facilities will make the reductions, can have this result as well. See *infra* note 304 and accompanying text.

²¹³ See ENVIRONMENTAL POLICY TOOLS, *supra* note 181, at 24–25 (citing second generation strategies as “most cost-effective tools”); Stewart, *supra* note 29, at 32–33 (stating that second generation strategies could save “tens of billions of dollars” per year as compared to command-and-control methods).

²¹⁴ See ENVIRONMENTAL POLICY TOOLS, *supra* note 181, at 37 (stating that second generation strategies such as pollution charges, tradable emissions, or challenge regulations are best at “spur[ring] technological innovation”); see also SALZMAN & THOMPSON, *supra* note 30, at 47 (noting cap and trade programs encourage “innovative practices and technologies”).

²¹⁵ See ENVIRONMENTAL POLICY TOOLS, *supra* note 181, at 28 (discussing findings that technology specifications slow appearance of new technologies); Ackerman & Stewart, *supra* note 176, at 1336 (asserting that best available technologies do not encourage development of new strategies).

determinations.²¹⁶ This allows the technology to keep pace with rapidly changing industries.²¹⁷

The root of these programs' strengths—giving the regulated parties a greater role in choosing how reductions will occur and who will achieve them—can also be a source of weakness. The environmental experience shows that it is easier to keep track of a uniform technology than to police facility-specific pollution reduction strategies.²¹⁸ Second generation strategies encourage differentiation. They accordingly offer less in the way of strict accountability and enforceability and open the door to bad-faith attempts to game the system.²¹⁹ They work best where reliable monitoring technologies exist to measure actual pollution releases.²²⁰ They are less desirable in situations, such as with the control of toxic emissions, where assurance of pollution reductions is the primary concern.

Second generation strategies appear well suited to privacy protection in the digital economy. As was mentioned above, privacy injuries, while costly, are seldom “toxic,” so strict accountability may not be as critical. On the other hand, the cost of regulation looms

²¹⁶ See Ackerman & Stewart, *supra* note 176, at 1336–37 (noting delays often caused by litigation); see also JOHNSON, *supra* note 212, at 23 (noting producers can identify pollution control options more quickly than government can). They also reduce information-gathering costs. JOHNSON, *supra* note 212, at 23; see also Ackerman & Stewart, *supra* note 176, at 1336–37 (stating centralized determinations “impose massive information-gathering burdens on administrators”). In traditional command regulation, government must collect and analyze great amounts of data to determine existing control technologies and the nature of the regulated industry. In most second generation strategies, polluters conduct the detailed engineering and economic analyses to determine whether pollution controls are warranted. This decreases the costs since firms typically have better access to this information than regulators do.

²¹⁷ See ENVIRONMENTAL POLICY TOOLS, *supra* note 181, at 27, 37 (recognizing second generation approaches as more “adaptable” than first generation); Hirsch, *supra* note 202, at 639–52 (describing how second generation approaches have been used to regulate rapidly changing manufacturing operations).

²¹⁸ See U.S. GEN. ACCOUNTING OFFICE, ENVIRONMENTAL PROTECTION: CHALLENGES FACING EPA'S EFFORTS TO REINVENT ENVIRONMENTAL REGULATION 52 (1997) (discussing concerns about site-specific rulemaking); Steinzor, *supra* note 176, at 201 (stating “the benefits of negotiating reinvention on a site-specific basis are not worth the considerable resources” being spent).

²¹⁹ Steinzor, *supra* note 176, at 138–39 (stating that such open attitude can lead to “regulatory free-for-all” and manipulation of EPA's Project XL); see also Mark Seidenfeld, *Empowering Stakeholders: Limits on Collaboration as the Basis for Flexible Regulation*, 41 WM. & MARY L. REV. 411, 484 (2000) (providing further criticism of Project XL).

²²⁰ See ENVIRONMENTAL POLICY TOOLS, *supra* note 181, at 40, 43 (“[I]mproved monitoring capabilities have been used to promote flexibility and increase assurance.”).

larger here. Second generation strategies, which draw on firms' ingenuity in coming up with low-cost solutions, should prove less costly. They should also be more able to adapt to the rapid innovation and technological change that characterizes information-based businesses.²²¹ Finally, widespread industry and public sentiment against government intervention in the digital economy²²² may make second generation strategies more politically feasible than command-and-control regulations. The environmental experience suggests that second generation regulatory strategies hold the most potential for the digital economy.

Four of these second generation environmental regulatory methods show special promise for the protection of privacy. Regulators could apply an emission fee approach to the problem of spam. Further, the government could adapt regulatory covenants, pollution release and transfer registers, and government promotion of environmental management systems for use in enhancing informational privacy.

V. USING EMISSION FEES TO REDUCE SPAM

In contrast to command-and-control regulation, emission fee systems do not specify control technology or emissions limits. Instead, they require facilities to pay a price for each unit of pollution emitted.²²³ If set at the right level, a fee forces polluters to internalize the cost of their emissions and so provides them with an incentive to reduce them.²²⁴ A familiar example would be local "pay-

²²¹ See Samuelson, *supra* note 10, at 2 (stating key policy challenge in Digital Age is "how to craft laws that will be flexible enough to adapt to rapidly changing circumstances"); cf. SOLOVE ET AL., *supra* note 10, at xxvii (noting challenge of protecting privacy in current "era of rapidly evolving technology"); Litan, *supra* note 3, at 1045 (describing Internet environment as "fast-moving").

²²² TURKINGTON & ALLEN, *supra* note 3, at 428 (citing survey showing that 67% of public prefers industry self-regulation to a "federal government privacy commission").

²²³ Stewart, *supra* note 29, at 94. The emission fee approach is based on the pioneering work of the early twentieth century British economist A.C. Pigou and is often referred to as Pigouvian taxes. JOHNSON, *supra* note 212, at 17; SALZMAN & THOMPSON, *supra* note 30, at 46.

²²⁴ SALZMAN & THOMPSON, *supra* note 30, at 45. It is often difficult to assess the true cost of pollution and to set an emission fee that properly causes the polluter to internalize that cost. JOHNSON, *supra* note 212, at 27. William Baumol and Wallace Oates have accordingly suggested a different form of emission fee system in which the government would determine, in advance, the level of pollution reduction that it wants to achieve and then set the fee at the

as-you-throw” programs for disposal of household waste.²²⁵ The more each household throws away, the more it has to pay. This creates an incentive to reduce household waste. According to one study, such policies led households to cut their waste nearly in half.²²⁶ The emission fee approach has also been applied to industrial discharges. For example, facilities located in regions with the worst smog problem pay a fee of \$5000 per ton of ozone-forming air pollutants emitted.²²⁷ The fee provides firms with an economic incentive to reduce but does not indicate *how* to do so, leaving it to the firms to develop the most cost-effective ways of achieving this.

Companies that figure out how to decrease their pollution for less than the price of the fee achieve a competitive advantage over rivals who are left paying the fee.²²⁸ The more such companies reduce their pollution, the more this advantage grows. This creates an on-going incentive to develop more cost-effective pollution control strategies.²²⁹ Such policies should promote innovation better than command-and-control regulations.²³⁰ They should also reduce regulatory costs. Instead of requiring all facilities to achieve the same pollution rate, as command-and-control regulations do, emission fees allow high-cost reducers to pay the fee and continue to emit, while giving low-cost reducers the opportunity to save money by decreasing emissions and avoiding the fees.²³¹ As a result, under

level that would lead to that level of reduction. *Id.*

²²⁵ JOHNSON, *supra* note 212, at 41. For a description of such programs, see *id.* at 41–42.

²²⁶ NAT'L CTR. FOR ENVTL. ECON., THE UNITED STATES EXPERIENCE WITH ECONOMIC INCENTIVES FOR PROTECTING THE ENVIRONMENT 44 (2001); see also JOHNSON, *supra* note 212, at 42 (discussing study).

²²⁷ Clean Air Act § 85, 42 U.S.C. § 7511d(b) (2000). European countries have made more extensive use of emission fees to reduce industrial pollution. JOHNSON, *supra* note 212, at 34–35. “France, Germany, and other countries impose taxes on the discharge of wastewater or other water pollutants.” *Id.* at 34. Sweden imposed a tax based on the sulfur content of fuel oil, which caused a 30% reduction in sulfur content during the first two years of its implementation. *Id.* at 35; Stewart, *supra* note 29, at 114. Sweden’s tax on emissions of nitrogen oxide resulted in a 40% reduction within two years. Stewart, *supra* note 29, at 114.

²²⁸ Adam Chase, *The Efficiency Benefits of “Green Taxes”: A Tribute to Senator John Heinz*, 11 UCLA J. ENVTL. L. & POL’Y 1, 11–12 (1992); accord JOHNSON, *supra* note 212, at 19–20; Stewart, *supra* note 29, at 99.

²²⁹ JOHNSON, *supra* note 212, at 19, 24; see also Stewart, *supra* note 29, at 100 (stating that managers, rather than government officials, are better situated to reexamine processes and to develop more resource-efficient methods).

²³⁰ JOHNSON, *supra* note 212, at 19, 24.

²³¹ Chase, *supra* note 228, at 11–12; Stewart, *supra* note 29, at 99.

an emission fee system, the low-cost reducers make the bulk of the reductions. This can yield “large cost savings for society as a whole”²³² and so can allow society to achieve better environmental quality at a socially tolerable cost.²³³

One downside of emission fee systems is that, by allowing facilities to choose their own control method, they make it harder for government officials to track emission levels and to enforce the fee requirements.²³⁴ Accurate real-time monitoring of emissions can address this shortcoming if such technologies are available.²³⁵ Such systems also run into difficulty in trying to match the fee to the actual costs of pollution, which can be hard to quantify.²³⁶ This failure to match can lead to over-control, if the fee is set too high, or under-control, if it is set too low.²³⁷

A. AN EMISSION FEE SYSTEM FOR SPAM

Government could implement an emission fee system for reducing spam by charging a fee per email sent. The fee should be equivalent to the damage that the spam email causes. This can be measured as

²³² Stewart, *supra* note 29, at 95. It may even lead to more efficient allocation of resources since the party will only continue to create the externalities and pay the associated fees where the value of its activities exceeds their full social cost. JOHNSON, *supra* note 212, at 18 (quoting Chase, *supra* note 228, at 11–12) (noting that when tax imposed equals marginal social cost of emissions, efficiency is achieved).

²³³ Other advantages of an emission fee approach, relative to a command-and-control approach, include (1) having companies, rather than government, make the complex design and engineering decisions that go into developing pollution controls, as firms can make these decisions more quickly and cheaply than the government can; (2) avoiding the large administrative costs associated with government decisionmaking of this type; and (3) avoiding the delays associated with the promulgation and legal defense of government technology specifications. See JOHNSON, *supra* note 212, at 23–24 (describing these advantages).

²³⁴ *Id.* at 29.

²³⁵ See ENVIRONMENTAL POLICY TOOLS, *supra* note 181, at 26 (“[M]onitoring capabilities . . . can provide a high degree of assurance.”).

²³⁶ JOHNSON, *supra* note 212, at 25–29; Orts, *supra* note 176, at 1243, 1269–70. This may be easier in the spam context than in the environmental one. The costs imposed by spam—such as time spent deleting emails, costs of filtering devices, increased user fees from ISPs, etc.—are more concrete than injuries to human health and the environment, which tend to involve greater uncertainties. Thus, it may be more possible to develop an accurate assessment of the costs of spam and to link it to a specific emission fee.

²³⁷ JOHNSON, *supra* note 212, at 27; see Lisa Heinzerling, *Selling Pollution, Forcing Democracy*, 14 STAN. ENVTL. L.J. 300, 305–10 (1995) (describing debate about how to best set emissions permit limits).

a function of the time spent deleting the message, the cost of filters used to capture it, the inconvenience caused by the loss of improperly filtered or deleted emails, and the payment of higher fees for Internet service.²³⁸ Additional research will be required to determine what this amount should be. For the present purposes, assume that the fee is one-tenth of a cent per email.²³⁹ A spammer sending one million messages a day would now have to pay \$1,000 per day, or \$365,000 per year, for a privilege that previously had been far less expensive.²⁴⁰ This could give them an incentive to better target their products to individuals who might actually be interested in them.²⁴¹ Internet marketers who figured out targeting methods that cost less than the price of the fee would gain an advantage over competitors who did not.²⁴² The more they narrowed their email distribution, the greater this competitive advantage would grow.²⁴³ This fee should drive socially beneficial innovation.

²³⁸ See *supra* notes 88–94 and accompanying text.

²³⁹ One report has suggested that a fee of 0.08 cents could be effective. Kraut et al., *supra* note 152, at 38.

²⁴⁰ See Zhang, *supra* note 87, at 304 (“Spammers are able to generate such a large amount of profit because there is no per-message charge for every piece of spam sent. Instead, a spammer’s overhead costs are negligible and confined to equipment, monthly rental fees for an email account, if any, and sometimes the price of a mailing list.”). Some organizations offer to deliver one million email messages for \$190, so that the cost of sending spam through an intermediary is 0.019 cents per message. ABADI ET AL., *supra* note 145, at 2. Given that the intermediary will build a profit margin into this price, the actual cost to the sender should be less than this amount.

²⁴¹ ABADI ET AL., *supra* note 145, at 14 (stating that charging small price for email would “clearly cause the demise of the more absurd sorts of spam, since the economic model would no longer support mailings with extremely low response rates”); Kraut et al., *supra* note 152, at 16 (stating that sender who has to pay price for email will target them better, “sending them only to those recipients for whom the benefit of sending the messages is more than its cost,” and reporting on equations that support this conclusion); Robert E. Kraut et al., *Markets for Attention: Will Postage for Email Help?* (Yale Int’l Cntr. for Fin., Working Paper No. 02-28, 2002) (reporting laboratory experiments showing that charging email postage causes senders to be more selective about sending messages and to send smaller number of messages).

²⁴² It is worth noting that, in order to target messages better, email advertisers may require access to more personal information about potential customers in order to know whether they might be interested in the specific product. Reducing spam through improved targeting of messages may thus be in tension with the desire to improve informational privacy. Society will have to decide how it wants to balance these competing priorities. The regulatory tools discussed in this Article will give it the means to do so. That should be an improvement over the current situation in which both spam and the use of personal information are headed towards a tragedy of the commons. See *supra* notes 145–69 and accompanying text.

²⁴³ See Chase, *supra* note 228, at 11–12 (describing concept in terms of environmental regulation).

It should also cause a weeding out of the email messages with the smallest value to recipients in favor of those with the most,²⁴⁴ because the senders of the latter would get a greater return and be more able to bear the fee. The email fee system would accordingly lead to more efficient allocation of inbox space. The closest analogy from the environmental field would be “congestion fee” systems that operate to reduce traffic congestion during peak commuting periods.²⁴⁵ These systems charge an extra fee for using busy roads during the traditional morning and evening commuting times.²⁴⁶ They seek to impose on the driver the “significant negative externalities she imposes upon society in the form of slowing down other motorists, poorer air quality, added noise, and wasted fuel resulting from idling,”²⁴⁷ and thereby cause some to shift to mass transit, carpooling, or other practices that minimize these externalities.²⁴⁸ The email fee system would be similar although it would alleviate inbox, rather than highway, congestion.

Several objections to this proposal should be addressed. *Would the email fee system deter socially beneficial communication among friends and family, within an organization, or by nonprofits that have limited funds?* Assuming that the average person sends 100 email messages per day to friends and family, the daily cost to each individual would be ten cents.²⁴⁹ Most should be able to afford this. In order to make the service free to most Americans, the government could allow individuals to claim a credit on their income tax return,

²⁴⁴ The point should not be to prevent all commercial email. Rather, it should be to increase the percentage of such messages that the recipients find valuable and decrease the percentage of those that they find annoying. Cf. Frequently Asked Questions About Spam, <http://spam.abuse.net/faq> (stating that point is not to stop commercialization of Internet, but rather to “promote responsible commercialization of the Internet”) (last visited Oct. 25, 2006).

²⁴⁵ See Lior Jacob Strahilevitz, *How Changes in Property Regimes Influence Social Norms: Commodifying California’s Carpool Lanes*, 75 IND. L.J. 1231, 1244–45 (2000) (discussing congestion-pricing schemes), reprinted in JOHNSON, *supra* note 212, at 45.

²⁴⁶ *Id.*

²⁴⁷ *Id.*

²⁴⁸ *Id.*

²⁴⁹ Applying the fee to all senders of email has the virtue of administrative simplicity since it would avoid the highly difficult (and constitutionally fraught) task of identifying the line between spam and nonspam. It is also consistent with the basic approach being taken here since even valued email takes up some available inbox space and thus imposes some costs. Such messages differ from spam in that positive benefits of the message, as experienced by the recipient, outweigh these costs.

of no more than a specific amount, for money that they or their dependents spend on email “stamps” during the course of the year.²⁵⁰ With respect to messages that travel within an organization the solution is quite simple. The system would govern only messages that travel on the Internet. It would not cover intra-organizational email that travels on an internal server. Thus, such messages would not be subject to the fee. Finally, nonprofits, educational institutions, and other organizations that are exempt from federal taxation under § 501(c)(3) of the U.S. Tax Code²⁵¹ could be made similarly exempt from having to pay the federal email fee.²⁵²

Is a fee-for-email system technically feasible? According to a 2003 article jointly authored by researchers from MIT, the University of California, Microsoft, and Google, a “ticket server” could administer a postage account for individual email senders.²⁵³ When the person sent a message, the server would attach a virtual “ticket” to the message (analogous to a postage stamp) and would decrease that person’s account by the amount of the fee.²⁵⁴ The ISP would allow

²⁵⁰ Foreigners sending email to American recipients would not be able to benefit from this tax credit. Moreover, those living in and sending email from poor nations may find it significantly harder to afford the email fee. The system could inhibit the ability of such individuals to send email. It will be important to pay attention to this potential downside of the system and to carefully evaluate the magnitude of this effect.

²⁵¹ I.R.C. 501(c)(3), 26 U.S.C. § 501(c)(3) (2000).

²⁵² The creation of an exempt class of email senders raises the possibility that technologically advanced spammers could “hijack” the email accounts of these organizations and use them to send out spam email for free. At least one study concludes that such activity could be minimized by monitoring the amount of email sent and comparing it to historical messaging activity. See SONIA ARRISON, *CANNING SPAM: AN ECONOMIC SOLUTION TO UNWANTED EMAIL* 14 (2004), available at <http://www.pacificresearch.org/pub/sab/techno/2004/spam01-26-04.pdf> (discussing claim by developer of email stamp system that such monitoring could prevent spammers from undermining system in this way).

²⁵³ ABADI ET AL., *supra* note 145, at 2.

²⁵⁴ *Id.* at 4. Some spammers may be able to hijack an individual’s email account and use it to send spam email. They could potentially run up a large bill in email “tickets” for which the account holder would later be held responsible. One way to limit such abuse would be to keep a relatively low balance in an individual’s ticket account so that it would quickly run out if attacked by a spammer. In addition, as mentioned above, it may be possible to detect such behavior by comparing email activity to historic patterns in the account and then take measures to prevent the abuse. See ARRISON, *supra* note 252, at 14. Further work will be required to determine whether this solution is an effective one or whether some other technological fix is needed. The purpose of this Article is not to settle such implementation issues but rather to map out the broad contours of a possible regulatory solution.

recipients to see only emails that arrive with a valid ticket.²⁵⁵ All of this could take place with no noticeable delay.²⁵⁶

Would overseas spammers be able to evade the fee? How could the government assert jurisdiction over them? All email that travels on the Internet—whether it originates domestically or abroad—must pass through a series of routers²⁵⁷ in order to find its way to the recipient’s computer.²⁵⁸ At least one of the routers must be located sufficiently close to a recipient’s computer to allow a hardwire connection. Without this connection, it would not be able to ultimately pass the message on to that device. This means that the final router, through which foreign email must pass before it reaches the recipient, will almost always be on American soil²⁵⁹ and will be

²⁵⁵ ABADI ET AL., *supra* note 145, at 4–5. The precision with which a ticket server can make sure that spammers pay the fee for each email may even represent an improvement over environmental emission fee programs. As was mentioned above, the main weakness of second generation approaches, including emission fee systems, is that they make it harder to monitor and enforce compliance. *See supra* notes 218–20 and accompanying text. The ticket server eliminates this problem for spam since it reliably tracks all “emissions.” Enforceability is further strengthened by the fact that the server automatically subtracts from the spammer’s account without the need for a large enforcement bureaucracy. *Cf. JOHNSON, supra* note 212, at 30 (citing this as virtue of emission fee systems).

²⁵⁶ *See* ABADI ET AL., *supra* note 145, at 3–5, for a review of this process. A fuller description of the system is as follows: Individuals purchase “postage” that exists in an account on a ticket server. *Id.* at 2, 4. When an individual wants to send an email, it automatically sends a request to the ticket server for an attachment that constitutes the ticket. *Id.* at 3–4. At that point, the sender’s postage account is decremented by the value of the ticket. *Id.* at 4. The receiver of the email automatically invokes the server’s “cancel ticket” operation, which “verifies that the ticket is valid, and that it hasn’t been cancelled before.” *Id.* The ticket server database will record that this specific ticket is now cancelled. *Id.* The ISP ensures that recipients will only see messages from someone who successfully completed the operation. *Id.* If there is no postage in the sender’s account, the email will not appear in the recipient’s inbox. *Id.* Once the operation is completed successfully, the ticket server returns a message to the recipient indicating that this operation has been successfully carried out and asking whether the recipient wants to “refund” the ticket. *Id.* The receiver can opt to refund the ticket where the message itself is not spam. If he does so, the value of the ticket is added to the original sender’s account. *Id.* If not, the account retains the decrement that it initially incurred. *Id.*

²⁵⁷ Routers are switches that specialize “in the routing of packets” of information. PERRITT, *supra* note 70, at 5.

²⁵⁸ *See* R. Scot Hopkins & Pamela R. Reynolds, Note, *Redefining Privacy and Security in the Electronic Communication Age: A Lawyer’s Ethical Duty in the Virtual World of the Internet*, 16 GEO. J. LEGAL ETHICS 675, 686 (2003) (describing series of routers that connect email sender with email recipient).

²⁵⁹ *See* Ronald J. Mann & Seth R. Belzley, *The Promise of Internet Intermediary Liability*, 47 WM. & MARY L. REV. 239, 256–58 (2005) (explaining that destination ISP will generally be located in same state as recipient). A limited exception could exist where the computer is

subject to U.S. jurisdiction.²⁶⁰ The federal government could legally require the router's owner—generally, an ISP²⁶¹—to pass on to the recipient only those email messages that had a valid “ticket.”²⁶²

Would a government fee limit free speech and violate the First Amendment? At the heart of the First Amendment is a distinction between content-based and content-neutral government regulation of speech.²⁶³ The government cannot restrain speech based on its “message, its ideas, its subject matter, or its content.”²⁶⁴ However, it can limit speech if the regulation is content-neutral and is substantially related to an important government purpose.²⁶⁵ The fee-for-email system would be content-neutral because it would make no distinctions based on the viewpoint of the sender or the subject matter of the communication.²⁶⁶ Moreover, as Congress has expressly stated, there is a “substantial government interest” in reducing spam so as to preserve the convenience and efficiency of electronic mail.²⁶⁷ Therefore, a First Amendment challenge to a fee-for-email system would likely fail. In an analogous context, the

hardwired to a router in Mexico or Canada, but this will apply only to machines that are near the border. Another could exist where American users access the Internet through a foreign dial-up system. The expense of the long distance call increases the cost of this option, making it rare. Thus, it is fair to say that virtually all American email users have a hardwire connection to a router located on American soil.

²⁶⁰ See Yulia A. Timofeeva, *Worldwide Prescriptive Jurisdiction in Internet Content Controversies: A Comparative Analysis*, 20 CONN. J. INT'L L. 199, 201–02 (2005) (explaining that under principle of territorial jurisdiction, each “state has jurisdiction over property, persons, acts, and events within its territory”); see also RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW OF THE UNITED STATES § 402 (1987) (same).

²⁶¹ See PERRITT, *supra* note 70, at 7 (discussing Internet connection service providers).

²⁶² See *supra* notes 253–56 and accompanying text. Moreover, ISPs should be able to distinguish email messages from other data being transferred on the Internet because each email communication has a header that identifies it as email, is written in a specific language (SMTP), and generally passes through a specific router port.

²⁶³ ERWIN CHEMERINSKY, *CONSTITUTIONAL LAW* 902 (Aspen Publishers, 2d ed. 2002).

²⁶⁴ *Police Dep't of Chi. v. Mosley*, 408 U.S. 92, 95 (1972).

²⁶⁵ See CHEMERINSKY, *supra* note 263, at 902 (stating that content-neutral regulation is subject to “intermediate scrutiny”); see also *Turner Broad. Sys. v. FCC*, 512 U.S. 622, 642 (1994) (same).

²⁶⁶ See CHEMERINSKY, *supra* note 263, at 904–05 (defining content-neutrality). The exemption for the first 100 messages sent from each email account does not alter this. All senders, regardless of viewpoint or content, would benefit from this exemption. Similarly, the exemption for 501(c)(3) organizations would apply to all such entities, regardless of their viewpoint or the subject matter of their communications. Thus, even with these limited exceptions, the scheme as a whole remains content-neutral.

²⁶⁷ CAN-SPAM Act of 2003, 15 U.S.C.A. § 7701(a)(2), (4) & (b)(1) (West 2003).

Supreme Court has held that a sales tax on cable media was content-neutral and did not violate the First Amendment.²⁶⁸

B. A NEW PERSPECTIVE ON RECENT PROPOSALS

In February 2006, ISPs America Online (AOL) and Yahoo announced plans to charge corporate emailers between a quarter of a cent and one cent for “preferred” email delivery.²⁶⁹ Companies that pay the fee will bypass the ISPs’ stringent filters²⁷⁰ and, under AOL’s proposal, will have their messages marked as “certified.”²⁷¹ Those not paying the fee will retain the current less reliable delivery system. Two years earlier, Bill Gates floated a more ambitious idea, much like the idea this Article has suggested; Gates proposed charging a fee for each email sent.²⁷² He argued that this would change spammers’ incentives and would reduce spam.²⁷³ Yahoo and AOL similarly argue that their “preferred” email option will encourage companies that use it to better target their messages so as to get a return that justifies paying the fee.²⁷⁴

Gates’s proposal was met with a storm of protest.²⁷⁵ Internet marketers and advocates alleged that the scheme was really a way for Microsoft to reap large profits from the fees.²⁷⁶ Gates ultimately withdrew the proposal and has since proclaimed his company’s “firm[] belie[f] that monetary charges would be inappropriate.”²⁷⁷ Yahoo and AOL’s more modest proposal may well suffer a similar fate. Internet advertisers and advocates have charged that the proposed system will “kill[] the whole openness of the e-mail

²⁶⁸ *Leathers v. Medlock*, 499 U.S. 439, 440, 453 (1991).

²⁶⁹ Hansell, *supra* note 90.

²⁷⁰ *Id.*

²⁷¹ *Id.*

²⁷² Gregory M. Lamb, ‘*Nickel and Diming’ Across the Internet*, CHRISTIAN SCI. MON., Feb. 23, 2004, at 13. The Gates proposal would create an exception for those whom the email recipient had put on their personal “do not charge” list. *Id.*

²⁷³ *Make ‘em Pay*, ECONOMIST, Feb. 14, 2004, at 58.

²⁷⁴ Hansell, *supra* note 90.

²⁷⁵ Kevin Murphy, *Gates Backs Away from Postage Stamps Idea in Spam Vision*, COMPUTERWIRE, June 29, 2004, available at LEXIS.

²⁷⁶ Scott Shane, *In E-Mail Warfare, the Spammers Are Winning*, BALT. SUN, Mar. 14, 2004, at 1A (quoting advocate as saying that Gates’s plan is “just a Microsoft plan to make money”).

²⁷⁷ Murphy, *supra* note 275.

system” and have labeled it “repulsive.”²⁷⁸ In a remarkable coalition, the liberal Moveon.org and the conservative RightMarch.com have come together to blast the proposal and call on Yahoo and AOL to reverse course.²⁷⁹

Seeing these proposals in the context of the environmental experience offers a new perspective. The environmental lense shows that spammers, like polluters, create negative externalities.²⁸⁰ This suggests that it is fair to require them to bear the costs they are creating. To say otherwise is equivalent to arguing that smokestack industries have a right to pollute the air without having to pay for their pollution or that it would be fundamentally wrong to require commuters to pay for using the highways at rush hour because they previously could do so for free. Indeed, the environmental precedent suggests that we could view free email as a subsidy that, while initially necessary to establish this communications medium, has now become destructive. Compare this to the early policies that allowed free grazing on federal land in order to subsidize the raising of livestock. As excessive cattle began to exhaust the land, the government introduced grazing fees to limit wasteful use.²⁸¹ The same logic would suggest that it is time to end free email and require online advertisers and others to bear the true cost of their activities.²⁸² The reaction to the Gates and AOL/Yahoo proposals suggests that this perspective is largely missing from the debate over spam. The environmental experience—particularly the notion of negative externalities and the government’s role in addressing them—provides new insight into the issue.

²⁷⁸ Mike Musgrove, *Paid E-Mail Seen as Sign of Culture Change: Guaranteed Delivery Plans by AOL, Yahoo Viewed as Part of End to Openness*, WASH. POST, Feb. 7, 2006, at D5 (quoting Julian Haight).

²⁷⁹ Robert McMillan, *Political Rivals Unite Against Giants’ E-Mail Plan*, INFOWORLD DAILY, Feb. 23, 2006, available at 2006 WLNR 3176301.

²⁸⁰ See *supra* notes 145–48 and accompanying text.

²⁸¹ See JOHNSON, *supra* note 212, at 105–06 (describing move from free grazing to grazing fees).

²⁸² If the appeal is to settled practice, then the evidence once again supports the fee system. The federal government has long required that those who send snail-mail pay for postage. What is this but a fee that corresponds to the cost that the sending of a letter imposes on the public? Anyone who uses the phone lines also has to pay in order to make a call. A fee for email would be consistent with these historic practices.

It also offers lessons for program design. Under the environmental model, the government, not a private party, collects the emission fees. By departing from this model, Gates, AOL, and Yahoo opened themselves to the charge of profiteering. A proposal, such as the one recommended in this Article, that employs a government-imposed fee would stand on stronger footing. The environmental experience also suggests that Gates's more ambitious proposal was preferable to Yahoo and AOL's limited plan. The Yahoo and AOL proposal would not meaningfully change spammers' incentives and would allow them to continue sending free email if they chose not to opt for the "preferred" system. It would thus seek payments from those who send messages that have real value, while allowing the most abusive spammers to escape paying for the costs of their activities. It would also give the ISPs (AOL and Yahoo) an incentive to filter out more and more "spam" email so as to push business to pay for the certified status. Just as an emission fee system includes all sources of pollution, an email fee system should cover all sources of email. Gates was on the right track with his more ambitious idea, although he erred by proposing that Microsoft collect the fee.

VI. USING REGULATORY COVENANTS TO PROTECT INFORMATIONAL PRIVACY

The environmental experience can also provide insight into current efforts to protect informational privacy. In 1996 and 1997, the Federal Trade Commission (FTC) told the largest online businesses that if they did not do more to protect informational privacy, it would require them to do so.²⁸³ This caused AOL, Hewlett-Packard, IBM, and others to form the Online Privacy Alliance (OPA) and to develop, on their own, a set of industry guidelines for the collection, use, distribution, and security of personal data.²⁸⁴ As a result, the FTC held off on federal regulation.

²⁸³ Keith Perine, *The Persuader*, INDUS. STANDARD, Nov. 13, 2000, available at LEXIS.

²⁸⁴ *Id.*; see also Litan, *supra* note 3, at 1059 (stating that OPA initiative was "prompted by the threat of actual regulation"). The OPA Guidelines require all organization members to implement the following five measures: (1) adopt and put into practice a "policy for protecting the privacy of individually identifiable information" and encourage the adoption of such

Subsequently, it became apparent that the OPA Guidelines would not be sufficient. Only a hundred or so companies and associations joined the group, with major players such as Amazon.com and Lycos choosing to remain on the sidelines.²⁸⁵ Pressure has again begun to build for federal regulation, leading even the OPA to conclude that it has “come up short.”²⁸⁶

The FTC and OPA’s experiment was more significant than most realize. Viewed through the lense of environmental policy, it can be seen as a step, albeit an incomplete one, toward use of a second generation tool known as a regulatory covenant. The environmental experience suggests that regulatory covenants can be very useful in situations—such as the one that the privacy field currently faces—where society needs to regulate but wants to minimize interference with the regulated industry.²⁸⁷ A fuller understanding of environmental covenants shows how this instrument might be effectively employed to protect informational privacy.

Under the environmental covenant approach, government officials sit down with the regulated industry and hammer out an agreement on pollution reduction. The conversation usually takes place against a backdrop of threatened prescriptive (first generation) regulation.²⁸⁸ The government offers that it will not impose such requirements if an agreement is reached.²⁸⁹ Sometimes, the negotiation includes a respected environmental group that functions

policies by those organizations with whom they do business; (2) make sure that the privacy policy is “easy to find” and understand and that it states clearly the content, use, and distribution of the information being gathered and the choices available to individuals with respect to the collection, use, and distribution of their information; (3) provide individuals with a choice regarding how their information will be used that, at least, includes the ability to “opt-out” of such use; (4) take measures to assure data reliability and to avoid “data loss, misuse[,] or alteration”; and (5) implement procedures to assure that the data are “accurate, complete [.] and timely” and provide a mechanism to correct inaccuracies. See Online Privacy Alliance, Guidelines for Online Privacy Policies, <http://www.privacyalliance.org/resources/ppguidelines.shtml> (last visited Oct. 25, 2006).

²⁸⁵ Perine, *supra* note 283.

²⁸⁶ *Id.*

²⁸⁷ See *supra* notes 171–80 and accompanying text (describing how privacy field faces these competing, and somewhat contradictory, demands).

²⁸⁸ JOHNSON, *supra* note 212, at 258.

²⁸⁹ *Id.* at 259.

as a third-party observer but retains the ability to go public and discredit the process if it smells a “rat.”²⁹⁰

Industry has more input in developing a covenant than a command-and-control regulation, tending to make covenants more practical and workable from an industry point of view.²⁹¹ Covenants often take the form of pollution reduction benchmarks or performance goals, rather than specific, technology-based requirements, which leaves an industry with significant flexibility in determining how to achieve the objectives.²⁹² In addition, covenants often employ longer time frames that fit with the normal cycles of business planning and investment.²⁹³ These features make covenants attractive to regulated parties. Government can benefit too; it often seeks and obtains steeper pollution reductions than those that political realities would allow it to achieve through prescriptive regulation.²⁹⁴ This benefit can attract environmental and community group support. The covenanting approach thus follows “the rationality of consensus—based on Coasian bargaining principles.”²⁹⁵ It allows the parties to negotiate an arrangement that all view as superior to that which they would face without such an

²⁹⁰ See Stewart, *supra* note 29, at 61 (noting importance of having “all relevant social interests with a stake in the outcome [be] adequately represented at the bargaining table”).

²⁹¹ *Id.* at 82.

²⁹² *Id.* at 81–82.

²⁹³ See Daniel J. Fiorino, *Toward a New System of Environmental Regulation: The Case for an Industry Sector Approach*, 26 ENVTL. L. 457, 486 (1996) (stating that length of covenants “allow industry to take a long-term strategic perspective in their environmental planning”); Stewart, *supra* note 29, at 82 (revealing that covenants often specify “a fixed, normally multi-year period” in which industry must come into compliance). This longer time frame allows industry to research the most cost-effective way of achieving the end result and to undertake a longer term research and investment plan. Stewart, *supra* note 29, at 82. Government usually commits not to pass regulation during this time period unless it is urgently required. *Id.*

²⁹⁴ Stewart, *supra* note 29, at 82–83 (“In return for the flexibility and extended compliance schedule provided, government will generally insist on steep reductions.”); see also JOHNSON, *supra* note 212, at 236 (noting governments and environmental groups enter covenants because they can “obtain commitments . . . [for] greater protection for the environment than would be required under traditional command-and-control laws”). Industry often views this as the “price” of the increased flexibility, time, and control that it is receiving. Stewart, *supra* note 29, at 83. In addition, covenants can also allow government to achieve effective controls more quickly and at less administrative cost than traditional methods since the agreement does not have to go through protracted regulatory processes. *Id.*

²⁹⁵ Stewart, *supra* note 29, at 61.

agreement.²⁹⁶ In theory, it *must* yield such a result since the parties enter into environmental covenants voluntarily.²⁹⁷ Thus, any who did not benefit could theoretically withhold their consent.

The Dutch have been the leading practitioners of this method and their Energy Efficiency Benchmarking Covenant illustrates it well.²⁹⁸ International agreements on climate change required the Netherlands to reduce significantly its carbon dioxide (CO₂) emissions.²⁹⁹ Concerns about regulatory costs led regulators to employ the covenanting method rather than prescriptive regulation.³⁰⁰ They offered to sit down with the most energy-intensive industries to negotiate a reduction plan, and the industries, knowing that they would otherwise face direct regulation, embraced this opportunity.³⁰¹ The resulting covenant sets out a flexible approach to improving energy efficiency over an extended time frame,³⁰² covers over 80% of Dutch industrial energy use, and has already been credited with reducing CO₂ by more than five million tons per year.³⁰³

Covenants can allow the regulated industry to focus the reduction burden on those facilities that can achieve it at least cost, thereby avoiding some of the inefficiencies of uniform, prescriptive regulation.³⁰⁴ Their flexible, performance-based standards and longer time frames encourage business investment in cost-effective means of achieving environmental results.³⁰⁵ Covenants can

²⁹⁶ JOHNSON, *supra* note 212, at 235 (“In theory, everybody wins.”).

²⁹⁷ Stewart, *supra* note 29, at 81.

²⁹⁸ See Commissie Benchmarking, Energy Efficiency Benchmarking Covenant, <http://www.benchmarking-energie.nl> (Dutch government website providing information on covenant) (last visited Oct. 26, 2006). European governments and the Japanese have used covenants to a greater degree than the United States has. Stewart, *supra* note 29, at 80–81. The European Union has encouraged their use by member states and has published guidelines directing how they can be used. Stephen M. Johnson, *Economics v. Equity II: The European Experience*, 58 WASH. & LEE L. REV. 417, 442–44 (2001). As of the mid-1990s, member states in the European Union have entered into more than 300 agreements with industrial sectors, firms, and associations. *Id.* at 444.

²⁹⁹ See Commissie Benchmarking, *supra* note 298.

³⁰⁰ *Id.*

³⁰¹ *Id.*

³⁰² *Id.*

³⁰³ *Id.*

³⁰⁴ JOHNSON, *supra* note 212, at 240.

³⁰⁵ *Id.* at 236, 240; Stewart, *supra* note 29, at 81–82. Covenants should also reduce a government’s administrative costs since the government would no longer need to go through

accordingly represent “an important means of addressing the shortcomings of command-and-control.”³⁰⁶ The approach also has its weaknesses. One is the risk that industry will use political influence and closed-door discussions to negotiate “sweetheart” deals.³⁰⁷ Having a respected environmental group at the table can reduce this threat. The differentiation that comes from increased flexibility can also make it more difficult to enforce covenants than technology-based regulation.³⁰⁸ This difficulty is best addressed through effective monitoring of actual emissions, where this is possible, and by stiff penalties for noncompliance. Finally, the legal status of environmental covenants is still unsettled under U.S. law.³⁰⁹

The covenanting approach could be used to protect informational privacy. Just as the Dutch government was getting ready to regulate CO₂ emissions, the federal government is now considering actions to protect informational privacy.³¹⁰ This should give information-intensive industries a reason to seek a deal. The existence of respected privacy advocacy groups³¹¹ that might add ideas and credibility to the negotiation also augurs well. The conditions are right for the federal government to sit down with the industries that collect and use personal information and to negotiate protective measures that are also workable for business.

the process of identifying the “best” technology.

³⁰⁶ Stewart, *supra* note 29, at 80; *accord* JOHNSON, *supra* note 212, at 240 (“[R]egulatory contracting arguably redresses many of the traditional criticisms of command-and-control regulation.”).

³⁰⁷ Stewart, *supra* note 29, at 83.

³⁰⁸ *Id.* at 85; *see also* JOHNSON, *supra* note 212, at 259 (stating that voluntary agreements are often criticized for lack of “sufficient provisions to monitor compliance”).

³⁰⁹ JOHNSON, *supra* note 212, at 259 (“[T]he legal status of a voluntary agreement is ambiguous.”); *see also* Stewart, *supra* note 29, at 84–85 (presenting many questions that lack clear answers). There are open questions about who can enforce these agreements and what the remedies for breach should be. Stewart, *supra* note 29, at 84. For example, it is not clear whether a citizen has standing to enforce the agreement against industry. *Id.* Similarly, questions exist as to industry’s rights in the event that government does not abide by the agreement and issues prescriptive regulations: can industry bring suit based on the agreement? *Id.* Background principles of law are not yet well developed on these issues. At present, it is advisable to address such matters in the text of the covenant itself.

³¹⁰ R. Christian Bruce, *Look for Comprehensive Privacy Bill in Spring 2006, Senate Staffer Says*, 4 Privacy & Sec. L. Rep. (BNA) 1048 (Aug. 15, 2005); *see also* Perine, *supra* note 283 (describing growing consensus for regulation to protect online privacy).

³¹¹ The Center for Democracy and Technology is one such group. *See* Ctr. for Democracy and Tech., <http://www.cdt.org> (last visited Oct. 25, 2006) (providing information about this organization).

While the FTC and OPA took a tentative step in this direction, the environmental experience shows that they could have handled it better in several regards. First, FTC initiated the discussion but then allowed the OPA to develop the guidelines on its own.³¹² This resulted in standards that lacked an official imprimatur, were too friendly to industry, and ultimately lacked sufficient credibility and breadth.³¹³ Had the FTC followed the environmental model, it would have directly negotiated the standards with the OPA. Second, the FTC failed to follow through on its threat of prescriptive regulation for those companies that did not sign on to the agreement.³¹⁴ Thus, the members of the OPA took on commitments while their competitors faced none. Once again, this departed from the environmental model in which those who fail to participate in the covenant face prescriptive regulation. Finally, unlike environmental covenants, the FTC gained no power to enforce the guidelines. This left the Commission with no middle-ground course of action, forcing it to either remain passive or seek full regulation. Had the FTC and industry followed the environmental model more closely, they might have emerged with a more effective arrangement.

This discussion is not idle speculation. The Dutch have used covenants to protect information privacy, and their effort appears to be working much better. The Dutch Personal Data Protection Act of 1999³¹⁵ establishes the conditions under which it is lawful to process personal data,³¹⁶ mandates notice to the government before initiating certain data processing operations,³¹⁷ requires processors to share certain information with the data subject,³¹⁸ and imposes other protections. As an alternative to these requirements, the Act allows an industry sector to draw up a code of conduct for processing of personal data and to submit it to the Data Protection Agency.³¹⁹ If

³¹² See *supra* notes 283–86 and accompanying text.

³¹³ See *supra* notes 283–86 and accompanying text.

³¹⁴ See *supra* note 285 and accompanying text.

³¹⁵ Wet bescherming persoonsgegevens [Personal Data Protection Act], Stb. 3022 (2000) (Neth.), translated in http://www.dutchdpa.nl/downloads_wetten/wbp.pdf?refer=true&theme=purple.

³¹⁶ *Id.* ch. 2.

³¹⁷ *Id.* ch. 4.

³¹⁸ *Id.* ch. 5.

³¹⁹ *Id.* ch. 3, art. 25(1).

approved, compliance with the code is deemed compliance with the Act,³²⁰ and the Agency gains the right to enforce it through the imposition of civil penalties.³²¹ An approved code thus becomes a tailored compliance plan geared specifically to the “particular features” of the sector.³²² As of 2002, the agency had approved twelve codes of conduct covering such sectors as banking, insurance, direct marketing, health, and pharmaceutical research.³²³ By way of illustration, the code for financial institutions establishes industry standards for the use of personal data in assessing potential customers³²⁴ and in marketing³²⁵ and provides special protections for sensitive categories of personal data, such as health information³²⁶ or data related to criminal offenses.³²⁷ The rapid proliferation of these agreements suggests that both government and industry like them and that the public is accepting them. They show that covenants could play an important role in privacy protection.

A covenant governing the data mining industry might have helped our hypothetical American, Donna. As in the Dutch Code of Conduct for Financial Institutions, the government could have targeted health information for special protection. Backed by the threat of prescriptive regulation, it could have negotiated restrictions on the collection and sale of such data especially where it is tied to a specific individual. The data mining industry might have accepted this restriction in exchange for clear authorization to continue core features of its business, such as the selling of information for credit checks or marketing. Industry would be at the table and could communicate whether the strategy was workable, while the presence of a reputable privacy organization would promote accountability. The parties might well have arrived at an

³²⁰ *Id.*

³²¹ *Id.* ch. 10, art. 65.

³²² *Id.* ch. 3, art. 25(1).

³²³ Peter J. Hustinx, *Co-Regulation or Self-Regulation by Public and Private Bodies—The Case of Data Protection*, in FREUNDESGABE BULLESBACH 283, 285 (2002).

³²⁴ Dutch Data Prot. Auth., Code of Conduct for the Processing of Personal Data by Financial Institutions § 5.2, available at http://www.dutchdpa.nl/downloads_gedragscode/ged_banken_vzm.pdf?refer=true&theme=purple.

³²⁵ *Id.* § 5.4.

³²⁶ *Id.* § 6.1.

³²⁷ *Id.* § 6.2.

agreement that both protected Donna and provided the industry with sufficient latitude to prosper.

VII. USING PUBLIC DISCLOSURE TO PROTECT INFORMATIONAL PRIVACY

Another second generation environmental strategy—Pollution Release and Transfer Registers (PRTRs)—would also serve as a useful model for privacy protection. PRTRs inform the public about pollution releases from specific facilities, thereby giving these organizations an incentive to pollute less. For example, the Emergency Planning and Community Right to Know Act (EPCRA) requires companies annually to report the quantity of hazardous chemicals that they have released into the environment or transferred off-site.³²⁸ EPA incorporates this information into the Toxic Release Inventory (TRI), a national computerized database that is available to the public over the Web,³²⁹ and issues an annual report naming those facilities that have released the most toxic substances.³³⁰ No company wants to be near the top of this list.³³¹ Publication of the TRI accordingly creates a strong incentive for businesses to reduce their toxic releases and “ha[s] been credited with stimulating a dramatic reduction in on-site inventories and releases of toxic chemicals.”³³² Between 1988 and 1998, toxic releases reported on the TRI decreased by 45.3%.³³³ Notably, TRI

³²⁸ 42 U.S.C. § 11023(f)(1)(A)&(B) (2000) (defining toxic chemical threshold amounts); JOHNSON, *supra* note 212, at 197.

³²⁹ 42 U.S.C. § 11023(j); JOHNSON, *supra* note 212, at 197. The public can access the TRI data at <http://www.epa.gov/triinter/tridata/index.htm>.

³³⁰ JOHNSON, *supra* note 212, at 199.

³³¹ Disclosure of negative information about a company can lead to a decline in sales, loss of business goodwill, loss of relationships with companies that do not want to be associated with such a business, decline in stock prices, and low retention of employees. *Id.* at 210.

³³² Stewart, *supra* note 29, at 139; *see also* ENVIRONMENTAL POLICY TOOLS, *supra* note 181, at 36 (stating TRI has caused substantial drop in toxic air emissions). *See generally* Shameek Konar & Mark A. Cohen, *Information as Regulation: The Effect of Community Right to Know Laws on Toxic Emissions*, 32 J. ENVTL. ECON. & MGMT. 109 (1997) (discussing these effects).

³³³ JOHNSON, *supra* note 212, at 211. Similar programs exist at the state level. California’s Air Toxics “Hot Spots” Information and Assessment Act of 1987 requires facilities to report on their toxic air emissions. CAL. HEALTH & SAFETY CODE § 44340 (West 2006); *see also* JOHNSON, *supra* note 212, at 202 (describing program). The Massachusetts Toxics Use Reduction Act requires those facilities that use large quantities of toxic materials to provide an inventory of the chemicals that they use. The state government then publishes this inventory to the public

achieved this result without issuing a single, substantive requirement. Instead, it used information disclosure to encourage companies to come up with their own ways of improving environmental performance. In this sense, PRTRs are very much a second generation strategy.

Just as no smokestack company wants to be known as a big polluter, no information-based business will want to be known as one that has “spilled” large amounts of personal information. The incentives may be even stronger in the digital economy. Individuals often cannot choose which producers of industrial chemicals they will patronize. Yet they make direct choices about which credit cards they hold, where they bank, and which e-commerce sites they visit. Recent studies show that they will avoid companies that are more prone to data spills.³³⁴ This should make pollution release registries an effective tool for protecting informational privacy.

Such a federal program—which could be called the Data Release Inventory (DRI)—would require companies that collect and use personal information to report annually how much of it they released that year. As with the TRI, the report should include both intentional releases (e.g., transfers of information to affiliates or other third parties) and unintentional ones (e.g., data security breaches). It should provide these figures both as a single, total amount, and in disaggregated form broken out by whether the release was intentional or unintentional. Government officials would compile this information and publicize it on the Web along with an annual ranking of individual company performance. If the environmental experience is any guide, newspapers and advocacy groups would likely latch onto this data and broadcast it widely. This would create strong incentives to better protect this

and posts it on the Internet. MASS. GEN. LAWS ch. 21I, § 3(B) (2002); JOHNSON, *supra* note 212, at 202–03 (describing program).

³³⁴ See *Many Customers Sever Ties with Businesses After Breach Notice, Law Firm Survey Shows*, 4 Privacy & Sec. L. Rep. (BNA) 1214, 1214 (Oct. 3, 2005) (reporting that survey shows data security breach at business causes 19% of consumers to cease dealing with that company and causes 40% to consider doing so). This survey demonstrates that organizations “lose customers when a breach occurs,” and that means data security breaches directly impact corporate bottom lines.” *Id.* See also Larry Ponemon, *What Do Data Breaches Cost Companies? Beyond Dollars, Customers Are Lost*, 4 Privacy & Sec. L. Rep. (BNA) 1310, 1310 (Oct. 24, 2005) (revealing data security breaches increase loss of customers).

information.³³⁵ Indeed, a recent survey found that health care organizations that experienced a data security breach were not doing more to close the leaks because they anticipated that noncompliance would not lead to any “‘public relations or branding problems.’”³³⁶ A public listing of companies’ data protection performance would change this.

Such a system might have helped Donna. Credit card companies compete fiercely and will lose clients if they gain a reputation for poor protection of personal information. A DRI would have given Donna’s credit card company incentive to improve its data management and security efforts. This might well have protected Donna from the data spill and ensuing identity theft.³³⁷

By contrast, prescriptive regulation would prove extremely difficult here. Many businesses collect and use personal data. Government regulators would face a mammoth task in trying to learn enough to design and prescribe data management and security practices for them. Even if they could manage this, business and technological developments in these fast-evolving industries would soon render the standards obsolete. A second generation approach that takes advantage of firms’ ability to redesign their own operations would work much better.

VIII. GOVERNMENT SUPPORT FOR ENVIRONMENTAL MANAGEMENT SYSTEMS AS A MODEL FOR IMPROVING THE PROTECTION OF PERSONAL INFORMATION

³³⁵ The data security breach statutes that some states have recently passed have already begun to create such incentives. See, e.g., CAL. CIV. CODE § 1798.82 (2006) (requiring disclosure when business experiences data security breach); *California’s Breach Disclosure Law Causes Consternation, Questions for Privacy Officers*, 2 *Privacy & Sec. L. Rev.* (BNA) 1277 (Nov. 10, 2003). One weakness of these statutes is that they may generate so many notices the consumers begin to tune all of them out. *Id.* The DRI approach avoids this problem because it provides only one, well-publicized report per year that summarizes the relevant information. It also allows consumers to compare company performance by looking at a single document, which the breach disclosure statutes do not.

³³⁶ Todd Sloane, *Not So Confidential: Patients Have Reason to Be So Worried About Who Is Seeing Their Medical Records*, *MODERN HEALTHCARE*, Nov. 14, 2005, at 22.

³³⁷ See Eric Dash, *Lost Credit Data Improperly Kept, Company Admits: Files Used for Research*, *N.Y. TIMES*, June 20, 2005, at A1 (describing major data spill by credit card processor that resulted, in part, from credit card companies’ failure to monitor and enforce requirement that processor discard personal information immediately after transaction).

At the 2005 Summit Meeting of the International Association for Privacy Professionals, the chief privacy officer (CPO) of a Fortune 500 corporation stated that one of her first actions upon assuming the position was to ask for a copy of the firm's environmental management system (EMS) and adapt it for use in privacy protection.³³⁸ Many of the other privacy officers in the room did not appear to know what an EMS was.³³⁹ The CPO's action points the way to another second generation measure—government promotion of EMS—that could be adapted for use in protecting personal information.

To understand this protection, it is necessary first to know how the EMS has revolutionized environmental management.³⁴⁰ Traditionally, an environmental officer remained largely independent of other company departments.³⁴¹ She was responsible for environmental compliance but was not involved in core decisions about what products the company would manufacture or how it would produce them. Others would make these calls, largely without reference to their environmental effects. An EMS takes down the walls between departments and gets many employees involved in improving environmental performance.³⁴² It does this through a management system—a set of organizational practices and procedures—that links the environmental manager to other employees and gets them thinking about the environmental dimension of their jobs.³⁴³ For example, an EMS might get a product designer, who traditionally would not have thought much about the environmental consequences of a given design, to consider the

³³⁸ Harriet Pearson, CPO, IBM Corp., Remarks at the International Association of Privacy Professionals National Summit Broader Perspectives Track (Mar. 10, 2005).

³³⁹ *Id.*

³⁴⁰ For a helpful discussion of environmental management systems and how they are designed, see generally Christopher L. Bell, *The ISO 14001 Environmental Management Systems Standard: A Modest Perspective*, [1997] 27 ENVTL. L. REP. (Envtl. Law Inst.) 10,622 (Dec. 1997).

³⁴¹ JASON MORRISON ET AL., *MANAGING A BETTER ENVIRONMENT: OPPORTUNITIES AND OBSTACLES FOR ISO 14001 IN PUBLIC POLICY AND COMMERCE* 40 (Pac. Inst., 2000).

³⁴² *Id.*; see also Gunningham, *supra* note 189, at 356 (stating EMS can change “enterprise’s environmental protection culture”).

³⁴³ Paula C. Murray, *Inching Toward Environmental Regulatory Reform – ISO 14000: Much Ado About Nothing or a Reinvention Tool?*, 37 AM. BUS. L.J. 35, 47 (1999) (stating that under EMS approach “[e]very employee, at every level, must be accountable for environmental performance within the scope of his or her job responsibilities”).

environmental side of her decisions.³⁴⁴ It might lead her to substitute a nonhazardous raw material for a toxic one, thereby eliminating a hazardous waste stream that required expensive disposal. This could improve both the company's environmental performance and its bottom line.³⁴⁵ As the U.S. EPA has recognized, EMSs can enhance compliance, pollution prevention, and environmental results.³⁴⁶ EMSs also provide firms with a means to communicate their environmental commitment to shareholders, consumers, and the public at large.³⁴⁷ In 1996, the International Organization for Standardization established a voluntary standard, known as ISO 14001, for evaluating environmental management systems.³⁴⁸ Firms that certify that their EMS complies with the standard are entitled to adapt their existing logo to reflect their precise ISO certification.³⁴⁹ More than 90,000 organizations are now ISO 14001 certified.³⁵⁰

Just as an EMS improves environmental performance, a privacy-focused analogue—call it a Personal Information Management System (PIMS)—could protect informational privacy. The typical privacy officer, much like the traditional environmental manager, is compartmentalized in the privacy “box” and is often unable to affect the core, strategic decisions that are at the root of the company's privacy impacts. A PIMS would connect the privacy officer to other employees in the organization and allow her to work with them to improve the company's privacy performance. It would make her less of an internal compliance officer, who spends the day getting others to meet legal requirements, and more of a *manager* of others'

³⁴⁴ MORRISON ET AL., *supra* note 341, at 40.

³⁴⁵ Cf. EPA Position Statement on Environmental Management Systems and ISO 14001, 63 Fed. Reg. 12,094, 12,095 (Mar. 12, 1998) (discussing EPA's promotion of and generation of EMS's pollution prevention ideas).

³⁴⁶ U.S. EPA, DRAFT EMS ACTION PLAN FOR PUBLIC COMMENT 16 (Dec. 20, 1999) (copy on file with author).

³⁴⁷ See Murray, *supra* note 343, at 53 (stating EMS provides “the marketing and public relations benefits of independent evidence of environmental commitment”).

³⁴⁸ MORRISON ET AL., *supra* note 341, at ix–x; Murray, *supra* note 343, at 42–43.

³⁴⁹ See INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, PUBLICIZING YOUR ISO 9001:2000 OR ISO 14001:2004 CERTIFICATION 4 (2005), <http://www.iso.org/iso/en/iso9000-14000/certification/publicizing/index.html>.

³⁵⁰ See Press Release, ISO, Latest ISO Survey Confirms Integration of ISO 9001 and ISO 14001 with World Economy (Sept. 15, 2005), available at <http://www.iso.org/iso/en/commcentre/pressreleases/archives/2005/Ref967.html>.

privacy-related actions. This is what the CPO of the Fortune 500 company was trying to achieve when she adapted her firm's EMS for privacy purposes.

Had OmniData adopted such a system, it might not have sold Donna's health information to prospective employers.³⁵¹ Instead, the designer of this product might have paid more attention to privacy and focused instead on providing services that did not rely on sensitive medical information. For example, OmniData might be able to use its databases to deduce whether a prospective employee is the type who moves from job to job. Employers concerned about turnover might find such information to be even more valuable than knowing about the applicant's past illnesses.³⁵² Much like pollution prevention, such proactive planning would have prevented Donna's privacy-related harm.

In the environmental field, government has played an important role in encouraging and facilitating the use of EMSs. It reduces inspection frequency³⁵³ and enforcement penalties³⁵⁴ for organizations that adopt an EMS. It has also developed resources for firms interested in implementing an EMS.³⁵⁵ Government could play an even greater role in promoting the PIMS.³⁵⁶ It could help to develop the PIMS and explain its potential to industry. Government could even create a standard for evaluating PIMS and could issue certificates to those firms that meet it. None of these measures would require firms to adopt a PIMS or to take any other action.

³⁵¹ See *supra* notes 131–33 and accompanying text.

³⁵² It may be difficult to draw this line. Why should information about a potential employee's propensity for leaving a job be fair game but data about that person's health problems be out of bounds? It all depends on how society defines the amount of privacy that an individual has a right to expect. Government—the accountable representatives of the public—could properly claim a role in defining how to draw these lines. Under the PIMS approach outlined above, it would then be up to the regulated parties themselves to figure out how to implement and achieve these publicly defined goals.

³⁵³ For example, the Oregon Green Permits program offers reduced inspection frequency, among other benefits, as an incentive to encourage firms to adopt an EMS. See OR. DEPT OF ENVTL. QUALITY, THE OREGON GREEN PERMITS PROGRAM GUIDE 4–1 (2000) (setting out benefits of adopting EMS and participating in program).

³⁵⁴ See U.S. EPA, *supra* note 346, at 12–13.

³⁵⁵ These include publication of an EMS implementation guide, establishment of an EMS resource center, and the creation of a database of existing EMSs. *Id.* at 16.

³⁵⁶ The federal government would probably have to be in charge to avoid duplicative efforts and emerge with a single standard, although states could play a role in initiating this effort.

Instead, these second generation strategies would encourage these companies to internalize the goal of privacy protection and to come up with ways to achieve it. In the complex, fast-moving information economy, this strategy could be an effective way to enhance privacy protection.

IX. CONCLUSION

From the AOL/Yahoo proposal to the OPA Guidelines to the Fortune 500 company's adaptation of its EMS for privacy purposes, the information economy seems to be groping its way towards second generation strategies for protecting privacy. This Article has shown why this should be so. It has demonstrated that second generation strategies are well suited to regulate industries—such as those that make up the information economy—that undergo rapid change, face stiff competition, and have the capacity for socially beneficial innovation. This Article has also expressly identified and more fully explained the second generation strategies that these sectors need. It has shown how these regulatory tools could be most effectively employed to protect privacy.

Although command-and-control regulation is not the best fit for the information economy, we should not give up on government action to protect privacy. To the contrary, the information economy needs such initiatives. Without them, a tragedy of the commons threatens email, e-commerce, and other online activity. To borrow one final environmental analogy, regulators need to develop strategies that will allow for the “sustainable development” of the information economy.³⁵⁷ Such policies will support innovation and prosperity but will do so in a way that sustains the personal privacy on which the digital economy itself depends. Second generation environmental laws and policies offer valuable lessons for the design of this new regulatory framework and for the protection of privacy in the Information Age.

³⁵⁷ PERCIVAL ET AL., *supra* note 183, at 1108 (defining “sustainable development” as “development that occurs on a scale that does not exceed the carrying capacity of the biosphere”).