NELLCO
NELLCO Legal Scholarship Repository

Duke Law School Faculty Scholarship Series | Duke Law School

8-1-2007

Reining in the Data Traders: A Tort for the Misuse of Personal Information

Sarah Ludington
Duke University Law School

Follow this and additional works at: http://lsr.nellco.org/duke_fs

Recommended Citation
Ludington, Sarah, "Reining in the Data Traders: A Tort for the Misuse of Personal Information" (2007). *Duke Law School Faculty Scholarship Series.* Paper 100.
http://lsr.nellco.org/duke_fs/100

This Article is brought to you for free and open access by the Duke Law School at NELLCO Legal Scholarship Repository. It has been accepted for inclusion in Duke Law School Faculty Scholarship Series by an authorized administrator of NELLCO Legal Scholarship Repository. For more information, please contact tracy.thompson@nellco.org.

REINING IN THE DATA TRADERS: A TORT FOR THE MISUSE OF PERSONAL INFORMATION

SARAH LUDINGTON*

In 2005, three spectacular data security breaches focused public attention on the vast databases of personal information held by data traders such as ChoicePoint and LexisNexis, and the vulnerability of that data. The personal information of hundreds of thousands of people had either been hacked or sold to identity thieves, yet the data traders refused to reveal to those people the specifics of the information sold or stolen. While Congress and many state legislatures swiftly introduced bills to force data traders to be more accountable to their data subjects, fewer states actually enacted laws, and none of the federal bills were taken to a vote before the election in 2006. In large part, individuals remain powerless to discover the information a data trader holds about them, to discover what information was sold or stolen, to prevent data traders from using their personal information in unauthorized ways, or to hold data traders accountable for lax security.

The Article argues that a new common law tort should be used to force reform and accountability on data traders, and to provide remedies for individuals who have suffered harm to their core privacy interests of choice and control—choice about who may receive their information, control over the information revealed, and how the recipient of that information may use it. The Article examines the current legislative and common law regimes, concluding that there are no effective remedies for individuals who have suffered harm from data misuse. Given the ineffective legislative response to the security breaches of 2005, the Article argues that the existing scheme of common law privacy torts should be expanded to create a new tort for information misuse. The new tort borrows from existing privacy torts—in particular, the tort of appropriation—and existing privacy statutes, importing the Fair Information Practices from the Privacy Act of 1974 as a standard of care.

Copyright © 2006 by Sarah Ludington.

* Senior Lecturing Fellow, Duke University Law School. For their helpful conversations and comments—and unbounded encouragement—I thank Stuart Benjamin, Brandt Goldstein, Mitu Gulati, Peter Barton Hutt, Jennifer Jenkins, Joan Magat, Paul Otto, Jed Purdy, and Chris Schroeder. For their research assistance, I thank Brian Wilson and Robert Needham. A special thanks to James Boyle, for getting me started, and to Chad Ludington, who keeps me going.

I. INTRODUCTION 141
II. THE PROBLEM OF DEFINING THE PROBLEM 147
III. THE FAILURE AND LIMITATIONS OF LEGISLATIVE REMEDIES. 151
IV. THE EXISTING SCHEME OF PRIVACY TORTS 159
A. Intrusion Upon Seclusion 159
B. Public Disclosure of a Private Fact 162
C. False Light 165
D. Appropriation and the Right of Publicity 166
V. WHAT IS TO BE DONE? 171
A. Potential Defendants: "One who Collects, Stores, Analyzes, or Trades" 174
B. Information Protected: "Personal Information" 175
C. Standard of Care: "The Failure to Use Fair Information Practices" 180
1. The Choice Principle 181
2. The Notice and Access Principles 183
3. The Security Principle 184
D. Damages 186
VI. CONCLUSION 188
APPENDIX 1 191
APPENDIX 2 192

I. INTRODUCTION

A woman receives frightening letters and telephone calls from a parolee who learned her address and telephone number while processing insurance data in prison. A law student discovers that someone obtained his student loan data and used it to apply for and max out a credit card. A man purchases classical music CDs from an Internet retailer and starts to receive unwanted e-mail solicitations from vendors selling similar music. A woman fortuitously discovers that a data broker has included her personal information on a direct marketing list entitled "waist-watcher-status-spender."

This Article begins with the premise that individuals should have available remedies for the types of information misuse described in the first paragraph, but under the current system of privacy regulation—including industry self-regulation, legislation, and common law remedies—none of these victims have an easy or obvious claim[1]

1. *See generally* Joel R. Reidenberg, *Privacy Wrongs in Search of Remedies*, 54 HASTINGS L.J. 877 (2003) (discussing the inadequacy of remedies currently available to address privacy wrongs).

against the company that collected, sold, rented, exposed, or analyzed their personal information.[2]

There are several holes in the current regulatory scheme. First, there are no regulations governing most private "data traders." For the purposes of this Article, a "data trader" is any private entity that collects, stores, processes, sells, rents, or disseminates personal information, including, but not limited to, a data broker. Data traders may include businesses such as direct marketers, retail establishments, online businesses (including Internet service providers), service industries (such as travel agents), and data brokers—entities whose sole business is to collect, analyze, and trade personal information. For example, the direct marketing industry is free from government regulation of its data trading practices, with the exception of the Do-Not-Call list imposed by the Federal Communications Commission (FCC) in 2003.[3] Second, most types of personal information—including names, birthdates, addresses, telephone numbers, clickstream data,[4] travel details (flights, car rentals, hotels, train tickets) and transactional data (who bought what from whom, when, where, and how)—are unregulated, unless the data trader violates its own privacy policy, in which case the Federal Trade Commission (FTC) can hold the company accountable for unfair trade practices. Thus it is currently legal—in the sense that there is no penalty—for data traders to sell

---

2. For the purposes of this Article, personal information means any information relating to an individual, including name, home address, e-mail address, work address, credit card numbers, Social Security number, transactional data, clickstream data, travel itineraries, any unique identifier associated with personal information in a database, and digital personality profiles obtained by aggregating, analyzing, or "mining" personal information, when it is or can be used to uniquely identify, locate, or contact that person. Personal information is also commonly called personally identifiable information (PII) or personal data. *See* Wikipedia, Personally Identifiable Information, http://en.wikipedia.org/wiki/Personally_identifiable_information (last visited Sept. 29, 2006) (defining "personally identifiable information" to encompass any information that can be used by a third party to identify, find, or contact an individual); Center for Democracy and Technology, Privacy Rules for Access to Personal Data, http://www.cdt.org/security/guidelines (last visited Sept. 29, 2006) (describing personal information as "personal data"). I have avoided the term "private information" because I believe that it is too restrictive, as it could be interpreted as information in which one has a subjective and objective expectation of privacy.

3. Press Release, FCC, FCC Authorizes Nationwide Do-Not-Call Registry (June 26, 2003), http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-235841A1.doc.

4. Clickstream data is

> a record of a user's activity on the Internet, including every Web site and every page of every Web site that the user visits, how long the user was on a page or site, in what order the pages were visited, any newsgroups that the user participates in and even the e-mail addresses of mail that the user sends and receives. Both ISPs and individual Web sites are capable of tracking a user's clickstream.

Webopedia, Clickstream, http://www.webopedia.com/TERM/C/clickstream.html (last visited Sept. 29, 2006).

personal information without the consent of the subject, to deny individuals information about the quantity or categories of lists that contain their information, and to deny any requests to remove personal information from these lists.[5] Even regulated data traders, such as banks and credit reporting agencies, are permitted to share personal information with their "affiliates"[6] without permission from the affected individuals.[7]

The problem of information misuse has grown with the data industry. Data traders collect, combine, analyze (or "mine"),[8] rent, and sell personal information in astonishing volumes. There are more than 1,000 data brokers in the United States,[9] the largest of whom claim to have detailed data profiles of "nearly every American consumer and household,"[10] and whose profits exceed $1 billion annually.[11] In 1992, it was estimated that data traders exchanged personal information every five seconds.[12] Since then, rapid advances in the

---

5. William J. Fenrich, *Common Law Protection of Individuals' Rights in Personal Information*, 65 FORDHAM L. REV. 951, 956 (1996). Not much has changed since Fenrich wrote his article, with two exceptions. The Gramm-Leach-Bliley Act (GLBA) requires financial institutions to provide notice regarding disclosure of personal information. 15 U.S.C. §§ 6802–6803 (2000). The revisions to the Fair Credit Reporting Act (FCRA) force credit institutions to disclose consumer reports to individuals. 15 U.S.C. § 1681a(d)(2)(A)(iii).

6. An "affiliate" is "any company that controls, is controlled by, or is under common control with another company." 12 C.F.R. § 216.3(a) (2006).

7. For example, the FCRA provides that

> "[C]onsumer report" does not include . . . any communication of other information among persons related by common ownership or affiliated by corporate control, if it is clearly and conspicuously disclosed to the consumer that the information may be communicated among such persons and the consumer is given the opportunity, before the time that the information is initially communicated, to direct that such information not be communicated among such persons.

15 U.S.C. § 1681a(d)(2)(A)(iii). Similarly, the GLBA generally requires only that financial institutions provide notice to consumers before "directly or through any affiliate, disclos[ing] to a nonafilliated third party any nonpublic personal information." 15 U.S.C. § 6802(a). The Health Insurance Portability and Accountability Act of 1996 (HIPAA) permits the sharing of personal information with entities that provide "health care operations." 45 C.F.R. § 164.502 (2005). For marketing opportunities, HIPAA requires the health care provider to obtain consent (an "opt-in") from an individual before sharing her information. 45 C.F.R. § 164.508(a)(3).

8. "Data mining" has been defined as the "process of sifting through large repositories of data with the goal of discovering patterns, trends, and associations among the data." Andrew J. McClurg, *A Thousand Words Are Worth a Picture: A Privacy Tort Response to Consumer Data Profiling*, 98 NW. U. L. REV. 63, 63 (2003).

9. *Id.* at 65.

10. *Id.*

11. *Id.* at 72.

12. Gregory Shaffer, *Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting Up of U.S. Privacy Standards*, 25 YALE J. INT'L L. 1, 2 (2000).

technology of data transfer and collection[13]—cookies[14] and spyware,[15] to name a few—have undoubtedly caused that rate to increase. Not coincidentally, reports of sales of personal information to thieves and security breaches in data banks have also increased. [16] According to the FTC, ten million Americans experienced some form of information misuse in the year 2002.[17] The estimated cost of that misuse to businesses, mostly financial institutions, was $50 billion.[18] In addition, the average individual paid $500 as a result of the misuse of his information and spent thirty hours resolving the problems caused by the misuse. [19]

Among academics, the debate about protecting personal information has mostly focused on the pros and cons of creating an individual property right in personal information.[20] This debate, when

---

13. McClurg, *supra* note 8, at 85–87 (describing new technology designed to allow disparate companies to exchange personal information more easily).

14. A "Web cookie" or "HTTP cookie" is text exchanged between a server and a user's web browser every time the user accesses that server. Wikipedia, HTTP cookie, http://en.wikipedia.org/wiki/Cookie_%28computer%29 (last visited Sept. 30, 2006).

15. The term "spyware" includes any software that records and disseminates information about a user's computer activity without that user's knowledge. Wikipedia, Spyware, http://en.wikipedia.org/wiki/Spyware (last visited Sept. 30, 2006).

16. R. Bradley McMahon, *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, 625 (2004).

17. SYNOVATE, FEDERAL TRADE COMMISSION—IDENTITY THEFT SURVEY REPORT 13 (2003), http://www.ftc.gov./os/2003/09/synovatereport [hereinafter SYNOVATE REPORT]. These information misuses occurred when perpetrators opened new credit accounts; acquired new loans; substituted the victim's name and identifying information when responding to a criminal investigation, renting an apartment, or obtaining medical care; misused victims' existing credit cards; and misused victims' existing checking, savings, or telephone accounts. *Id.* at 4.

18. *Id.* at 6. The *Synovate Report* does not allocate the costs of information abuse among different types of businesses, but the types of misuses described in the *Synovate Report* are primarily connected with financial institutions. *Id.* at 4–7.

19. *Id.* at 6; *see also The Story: "Who Am I?"* (American Public Media radio broadcast, Oct. 2, 2006) (audio file available at http://the story.org/archive/the_story_79_Who_Am_I.mp3/mediafile_view) (chronicling the Sisyphean efforts of one woman to cope with the emotional and financial havoc wreaked by identity theft).

20. *See, e.g.*, Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1428–36 (2000) (proposing legislation that creates a limited property right of informational privacy); Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 HARV. L. REV. 2056, 2056, 2094 (2004) (developing a model of "propertized personal information" that (1) limits alienability of personal information; (2) establish opt-in default rules; (3) creates a right to rescind data trade agreements; (4) confers liquidated damages to successful litigants to effectively deter violations; and (5) defines institutional roles in regulating the information market); Daniel J. Solove & Chris Jay Hoofnagle, *A Model Regime of Privacy Protection*, 2006 U. ILL. L. REV. 357, 368–82 (proposing a regulatory model for privacy protection that emphasizes individuals' control over their personal information).

not mired in formalist notions of privacy,[21] has proposed some innovative protections for information privacy. However, all rely on a legislative agenda to create and enforce a property regime in personal information.[22] Regrettably, the legislative will to construct such a regime does not exist, as the data breaches of 2005—and the lack of a comprehensive legislative response—made painfully clear.[23]

In the absence of effective legislation, the common law currently offers few remedies to individuals whose data are misused. Contract solutions have failed because it is difficult for consumers to police the privacy agreements of the companies with which they do business, if those companies have privacy agreements at all.[24] Scholars who have considered a tort remedy for information misuse have mostly concluded that the existing scheme of privacy torts is inadequate.[25] Andrew McClurg has argued for the usefulness of tort law in addressing the misuse of personal information. [26] But, like many scholars who advocate a property regime, he focuses on the nonconsensual collection or selling of information, hoping that tort liability will "deter nonconsensual data profiling,"[27] without considering remedies that address the way data traders analyze, use, and misuse the information

---

21. *See, e.g.*, Schwartz, *supra* note 20, at 2095 (questioning whether information property should be viewed as a bundle of sticks or as an exclusivity axiom).

22. *See, e.g.*, Cohen, *supra* note 20, at 1377 (endorsing legislative efforts to protect private information); Schwartz, *supra* note 20, at 2119 (same); Solove & Hoofnagle, *supra* note 20, at 358 (proposing legislation for privacy protection); *see also* Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1287–94 (1998) (proposing legislation for cyberspace privacy protection, without defining information privacy as a property right).

23. *See infra* Part III.

24. *See* Eugene Volokh, *Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People From Speaking About You*, 52 STAN. L. REV. 1049, 1057–62 (2000) (discussing the limitations of using contract law to protect private information); *see also* Susan M. Gilles, *Promises Betrayed: Breach of Confidence as a Remedy for Invasions of Privacy*, 43 BUFF. L. REV. 1, 25–32, 38–39 (1995) (explaining why contract law rarely provides an effective remedy for dissemination of personal information).

25. *See, e.g.*, Robert Gellman, *Does Privacy Law Work?*, *in* TECHNOLOGY AND PRIVACY: THE NEW LANDSCAPE 193, 209–11 (Philip E. Agre & Marc Rotenberg eds., 1997) (asserting that tort remedies do not adequately redress privacy invasions advanced by newly developed technologies); A. Michael Froomkin, *The Death of Privacy?*, 52 STAN. L. REV. 1461, 1510 (2000) (discussing the constitutional and practical limits to using tort law to regulate invasive new technologies); McClurg, *supra* note 8, at 97 (noting scholars' pervasive disbelief that tort law could practically regulate data trading); James P. Nehf, *Recognizing the Societal Value in Information Privacy*, 78 WASH. L. REV. 1, 29–32 (2003) (asserting that tort law was not designed to address modern technological invasions of privacy and is an ineffective tool to prevent or redress injuries resulting from data trading).

26. *See generally* McClurg, *supra* note 8 (advocating use of the tort of appropriation to deter invasive data trading practices).

27. *Id.* at 101. *But see generally* Tal Z. Zarsky, *Desperately Seeking Solutions: Using Implementation-Based Solutions for the Troubles of Information Privacy in the Age of Data Mining and the*

that they have collected with the data subject's permission, or that is available for use in public records.[28]

This Article suggests that a new common law tort could be used to provide remedies to people harmed by common types of data misuse, as suggested by the four hypotheticals in the first paragraph: insecure data practices—such as allowing felons to process personal information, or releasing personal information data to identity thieves—and the use of personal information data for purposes extraneous to the original transaction—such as renting it to a vendor of related products, or mining it to create a consumer profile or direct marketing list. Tort liability for data misuse would provide incentives for data traders—the entities who are in the best position to prevent the harms of data misuse—to discover, and honor, the privacy choices of individuals. While a legislative solution is ultimately preferable, a tort solution is a time-honored fix for harms that the legislative process has manifestly failed to address.

The new tort, when placed in the context of existing privacy torts and statutory schemes, is less of a new tort than a cautious expansion of the old torts into areas created by the technological revolution of the past century. Like the appropriation tort, the new tort remedies the harm to an individual caused by his loss of control over his identity. Like the Privacy Act of 1974 (Privacy Act),[29] the new tort uses the four principles of Fair Information Practices—notice, choice, access, and security [30]—as the minimum standard for acceptable data management. The tort charts new ground in expanding the definition of what is considered private, in targeting commercial uses of data, and in transferring the principles of Fair Information Practices from the public sector to the private sector.

Part II of this Article conceptualizes and defines the harm caused by information misuse. Part III examines the limitations and failures of the current legislative regime, focusing in particular on the ineffective legislative response to information privacy breaches in 2005. Part IV explores in detail the current scheme of privacy torts, and why it is ill-equipped to address information misuse. Part V proposes the new cause of action and outlines its elements. Part VI concludes by ad-

---

Internet Society, 56 ME. L. REV. 13 (2004) (focusing on solutions that address the implementation stage of the data flow).

28. *See* Nehf, *supra* note 25, at 17–19 (describing how the development of vast government databases that are online and open to inspection by the public has aided the direct marketing industry).

29. Privacy Act, 5 U.S.C. § 552a (2000 & Supp. 2006).

30. *See, e.g.*, *id.* § 552a(e) (notice); *id.* § 552a(b) (choice); *id.* § 552a(d) (access); *id.* § 552a(e) (security).

dressing some of the objections and criticisms that may be leveled at this proposal.

II. THE PROBLEM OF DEFINING THE PROBLEM

One reason that the law has been slow to devise effective remedies for information misuse is that a consensus on the harm it causes has not yet emerged. Consider the examples given in the first paragraph of this Article. The harms described range from the obvious—stalking and identity theft—to the abstruse—psychological distress at the loss of control over the use of one's information, or humiliation and loss of dignity at being categorized into demeaning consumer profiles. While most people would agree that identity theft and stalking cause harms that deserve remedies, junk e-mails and demeaning epithets cause psychological or intangible harms that can more easily be ignored, ridiculed, or minimized. Indeed, consumers may view unwanted targeted advertising, like the unsolicited advertisements for classical music CDs, as a necessary annoyance—part of what consumers "pay" for the convenience of online shopping or receiving discounts at the grocery store.

Despite the range of consumer preferences for information privacy, there is still a coherent theoretical basis for the harm caused by information abuse. The harm is properly conceptualized as an injury to autonomy, as the right of information privacy is defined (somewhat paradoxically)[31] as an individual's right to control her public image, including the ability to choose what she reveals and what she keeps hidden.[32] Choice and control are core privacy values, and they are themes evident in the earliest to the most recent writings on privacy. Warren and Brandeis, for example, complained about the "unauthorized circulation of portraits of private persons,"[33] and praised the common law of copyright, which empowers the individual to control whether and when "that which is his"—including his letters, drafts, or

31. James Q. Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 YALE L.J. 1151, 1168 (2004) (noting the paradox in American scholars' depiction of the right to privacy as a "right to a *public* image of our own making").

32. Kang, *supra* note 22, at 1205 (defining information privacy as "an individual's claim to control the terms under which personal information—information identifiable to the individual—is acquired, disclosed, and used"). Kang explicitly adopts the definition of information privacy developed by the Clinton Administration's Information Infrastructure Task Force in 1998, noting that the definition is similar to the one that informed the Code of Fair Information Practices and the Privacy Act of 1974. *Id.* at 1205–06 & n.43.

33. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 195 (1890).

diaries—"shall be given to the public."[34] Alan Westin identified the control of one's public persona as a key aspect of two of his four "functions" of individual privacy.[35] "Limited and [p]rotected [c]ommunication"—an individual's use of reserve and discretion in his communications with others—facilitates intimate relationships at home and work, and sets necessary boundaries in relationships.[36] "Personal [a]utonomy"—individual resistance to complete domination or manipulation by another—depends, in part, on a person's "sense that it is he who decides when to 'go public'" with his privately incubated ideas or views.[37]

In a similar vein, Jeffrey Rosen imagines the right of privacy as a bulwark against the misinterpretations and misjudgments that result when the most intimate details of a life are unexpectedly, and without permission, thrown into public view, in a world where "information can easily be confused with knowledge."[38] More recently, James Whitman connected the control theme with the core notions of privacy in continental Europe:[39] the rights to "one's image, name, and reputation, and what Germans call the right to informational self-determination—the right to control the sorts of information disclosed about oneself."[40]

Other writers have conceptualized the harm caused by the misuse of personal information as drastically dehumanizing and debilitating. Using metaphors derived from George Orwell and Franz Kafka,[41] Daniel Solove decries the creation of digital dossiers—extensive data profiles constructed through the aggregation and analysis of huge

---

34. *Id.* at 199; *see also* Roberson v. Rochester Folding Box Co., 64 N.E. 442, 449 (N.Y. 1902) (Gray, J., dissenting).

35. *See* ALAN F. WESTIN, PRIVACY AND FREEDOM 32 (1970) (identifying four core privacy functions).

36. *Id.* at 37–38.

37. *Id.* at 33–34.

38. JEFFREY ROSEN, THE UNWANTED GAZE: THE DESTRUCTION OF PRIVACY IN AMERICA 7–8 (2000). The fear of mischaracterization resulting from unauthorized dissemination of personal information may be particularly acute when individuals have little control over data traders' activities. *See* Nehf, *supra* note 25, at 26–27.

39. Whitman, *supra* note 31, at 1167–68.

40. *Id.* at 1161 (emphasis and footnote omitted). Whitman contrasts the European model with the American model of privacy, which, as expressed in the Fourth Amendment, is more concerned with freedom from state intrusion. *Id.* at 1161–62. While this Article focuses on private data traders, it is worth noting that data traders obtain much of their information from public databases, compile that information with consumer data, and then often sell aggregated data profiles to the government. DANIEL J. SOLOVE, THE DIGITAL PERSON 169–70 (2004). Thus, anti-statist concerns are implicated in reigning in the data traders, as the private sector is doing with information what the government has forbidden itself to do.

41. SOLOVE, *supra* note 40, at 7–9.

quantities of personal information, that particularly attempt to infer tastes, preferences, and habits based on consumer transactions.[42] According to Solove, these dossiers may "foster a state of powerlessness and vulnerability created by people's lack of any meaningful form of participation in the collection and use of their personal information."[43] Andrew McClurg similarly argues that a digital dossier "implicates a person's 'inner identity'" by attempting to replicate his very personality.[44] By appropriating this inner identity and assigning labels to it, data traders "steal[ ] something intimate and important that has been self-constructed," fundamentally robbing the consumer of the right to assign his own labels to himself.[45]

Professors Solove and McClurg may have overstated the harm, as their theories are belied by both empirical and theoretical objections. First, their theories ignore those consumers who are willing to trade their personal information for frequent flier miles, grocery store discounts, or the convenience of one-click shopping. Either these consumers are ignorant of or willfully blind to the danger of trading their information, or they instinctively perceive the risk as something less than a dire affront to their personhoods.

The theoretical basis of this instinct is the disjunction between what one purchases and one's perceived inner identity. Thus, while what we buy reveals much about who we are, or hope to be, it is also true that much of the personal data generated by consumer transactions does not reveal the inner identity of the consumer, and that the aggregation and profiling of this data does not necessarily cause the consumer to feel powerless and vulnerable. Granted, my own purchases reveal my real, perceived, or desired class status; my age, national, ethnic, religious, or gender identity; my tastes and preferences; and the hours I keep. But I equally doubt that someone who knows all these details knows me intimately or privately. Purchases of drugs or medicine get closer; reading and viewing choices draw closer still. Accordingly, a digital dossier might come close to describing my persona or even my personality, but ultimately and ironically, it misses my inner self: my thoughts, hopes, spirituality, relationships, and per-

42. *Id.* at 1–2.
43. *Id.* at 47–48.
44. McClurg, *supra* note 8, at 124–25.
45. *Id.* at 126.

sonal dignity. The closer data profiles come, the farther away they seem, and that irony can be both subversive and empowering.[46]

Rather than exaggerate the harm of information misuse, this Article asserts that information misuse is, at a minimum, an injury to the individual's autonomy—or rights of choice and control—which are indisputably core values of the right to privacy. An individual whose personal information has been sold, rented, or analyzed without his consent experiences injury precisely to his choice and control—choice over who may receive his information, and control over the information revealed and how the recipient may use it.

The harm is also usefully viewed as an injury to the individual as consumer, for whom choice and control are critical values. In a recent article, Stan Karas defines information privacy as "the protection of the integrity of the individual self as composed of a multitude of identities," including "the individual as a consumer," and argues that data use becomes intrusive if it "disclos[es] the subject's personality as expressed through his consumer self."[47] Karas connects consumption habits, self-expression, and identity,[48] arguing that an accurate and comprehensive record of our purchases can produce "a blurry but strikingly accurate glance" at our expressive, ergo private, selves.[49] Connecting Karas's notion of the privacy of the individual as consumer with the privacy value of autonomy suggests that data use becomes harmful if it compromises the choice and control of the consumer over the use of his personal information.

Viewed as an injury to the individual as consumer, the harm caused by information misuse looks less like a novel idea and more like a small part in the grander scheme of consumer injuries. The law already protects the individual as consumer with systems such as the product liability scheme, and comprehensive legislation designed to mitigate power imbalances between individuals and institutions and to make consumer credit and banking transactions transparent and fair. It makes sense, therefore, that the law would protect the individual vis-à-vis data traders, mitigating power imbalances and devising a system to make the trading and use of information more transparent and fair.

---

46. *See* ROSEN, *supra* note 38, at 9 ("But even if we saw the [clickstream] logs of everything she had read and downloaded this week, we wouldn't come close to knowing who she really is. (Instead, we would misjudge her in all sorts of new ways.)").

47. Stan Karas, *Privacy, Identity, Databases*, 52 AM. U. L. REV. 393, 429 (2002).

48. *Id.* at 424, 427–29.

49. *Id.* at 398.

III. THE FAILURE AND LIMITATIONS OF LEGISLATIVE REMEDIES

The current system—if it can be called one—for regulating the use of personal information by private data traders does so inconsistently and unpredictably.[50] Currently, federal legislation regulates the use of bank records,[51] cable TV records,[52] credit reports,[53] information about children collected through the Internet,[54] medical information,[55] educational records,[56] "consumer proprietary network information" (CPNI),[57] and video rental records,[58] but with varying degrees of strength and no comprehensive system of oversight. Additionally, various states regulate the use of insurance records,[59] library records,[60] Social Security numbers,[61] and telephone services.[62] Still, individuals whose data have been misused have few viable statutory remedies. Many federal privacy statutes do not include provisions that grant a private right of enforcement,[63] or provide such a low level of liquidated damages that litigating claims is not cost effective.[64] Public enforcement of privacy policies by the FTC and state attorneys gen-

---

50. Critics use a variety of unflattering epithets to describe the uncoordinated aggregation of industry self-regulations, and state, federal, and common laws that protect (or fail to protect) personal information. *See, e.g.*, *id.* at 401 ("patchwork"); Kurt M. Saunders & Bruce Zucker, *Counteracting Identity Fraud in the Information Age: The Identity Theft and Assumption Deterrence Act*, 8 CORNELL J.L. & PUB. POL'Y 661, 670 (1999) ("scatter-shot").

51. ROBERT ELLIS SMITH, COMPILATION OF STATE AND FEDERAL PRIVACY LAWS 7–8 (2002).

52. *Id.* at 9.

53. *Id.* at 17.

54. *Id.* at 44.

55. *Id.* at 50.

56. *Id.* at 63–64.

57. *Id.* at 69. CPNI is information pertaining to telephone services: "information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer . . . and information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer . . . ." 47 U.S.C. § 222(h)(1) (2000).

58. SMITH, *supra* note 51, at 44.

59. *Id.* at 36–39.

60. *Id.* at 40–41.

61. *Id.* at 60–61.

62. *Id.* at 67–69.

63. *E.g.*, Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. § 1232g (2000) (education records); Federal Trade Commission Act, 15 U.S.C. §§ 41–58 (2000) (unfair and deceptive trade practices); Identity Theft and Assumption Deterrence Act (ID Theft Act), 18 U.S.C. § 1028 (2000 & West Supp. 2006) (identification documents).

64. *E.g.*, Privacy Act, 5 U.S.C. § 552a(g)(4) (2000 & Supp. 2006) (granting $1,000 minimum recovery to plaintiffs who bring successful Privacy Act claims). Victims of identity theft are not compensated for their losses under the ID Theft Act. McMahon, *supra* note 16, at 632.

eral[65] has failed to reform the data traders or to effectively stem the incidence of identity theft.[66]

At the federal level, some of the more effective legislation is leveled at very narrow categories of data, but entire swaths of personal information are left unprotected. The haphazard creation of federal privacy legislation is perhaps best illustrated by the Video Protection Privacy Act (VPPA),[67] which prohibits a video store from releasing lists of rented or requested videos, except pursuant to legal process.[68] Any person whose information is released can sue in federal court and receive actual damages (not less than the liquidated sum of $2,500), punitive damages, and attorneys' fees.[69]

This (relatively) robust framework for the protection of privacy in video rental records is the ironic legacy of Judge Robert Bork, whose video rental records were obtained by and published in *City Paper*, a Washington, D.C. weekly, during the course of Judge Bork's contentious confirmation hearings for a seat on the Supreme Court.[70] The media initially reacted to the list with light-hearted commentary on the Borks' taste in movies (the consensus being that it was rather good).[71] A few days later, Senator Alan Simpson criticized *City Paper* for its "arrogant, smart-aleck, super-sarcastic, puerile, sorry and pathetic" article,[72] and the American Civil Liberties Union and People for the American Way—groups that actively opposed Judge Bork's

---

65. Public enforcement, which typically addresses unfair and deceptive trade practices, is limited to examining whether a data trader adheres to its own privacy and security policies. Reidenberg, *supra* note 1, at 886–87.

66. Identity theft is a federal crime and many states have passed laws specifically criminalizing identity theft. Daniel J. Solove, *Identity Theft, Privacy, and the Architecture of Vulnerability*, 54 HASTINGS L.J. 1227, 1246–47 (2003). Nevertheless, most of these statutes do not allow for individual remedies. *Id.* at 1247–48, 1250.

67. VPPA, 18 U.S.C. § 2710 (2000).

68. *Id.*

69. *Id.* The VPPA leaves open a loophole, allowing stores to sell to direct marketers lists of customer names and addresses, arranged by categories of videos rented (e.g., romantic comedy, schlocky western), unless a customer has specifically opted-out of this opportunity. Schwartz, *supra* note 20, at 2099 n.221.

70. *Of a Judge and His VCR*, UNITED PRESS INT'L, Sept. 26, 1987.

71. *See, e.g.*, *National Editorial Sampler*, UNITED PRESS INT'L, Sept. 30, 1987 (reporting one reviewer's assessment of the Borks' taste in movies as "impeccable"); *Of a Judge and His VCR*, *supra* note 70 (highlighting the Borks' selection of Washington-related movies); *Personalities*, WASH. POST, Sept. 26, 1987, at C3 (noting the Borks' preference for British movies and Cary Grant films).

72. *In the News*, ARK. DEMOCRAT-GAZETTE, Sept. 29, 1987. The *Washington Post* was quick to mock politicians, including Senator Simpson, who expressed anger over the release of Bork's video rental records. Editorial, *Invasion of Video Privacy*, WASH. POST, Sept. 30, 1987, at A18 (satirizing Judge Bork's video rental disclosure).

nomination[73]—jumped into the debate on the side of the judge and his right to keep his video rental records private.[74]

Thus were spawned the "son of Bork" bills—state and federal legislation that prohibited the release of video rental records.[75] But the Bork bill failed to engender similarly strong legislation to protect individuals against the misuse of other forms of personal information. Thus, while my video rental store may not release my rental records, a retail vendor of videos could sell or rent a list of my purchases, as can vendors of books, music CDs, or DVDs.

The haphazard legislative coverage of personal information can be viewed as a history of effective lobbying by the direct marketing industry, which has actively worked against government regulation of data trading. Almost thirty years ago, as a way of fending off legislatively forced reform, lobbying groups for data traders—including one of the key players, the Direct Marketing Association (DMA) (formerly Direct Mail Marketing Association)[76]—pledged to the Privacy Protection Study Commission that it would regulate itself.[77] To fulfill its obligation, the DMA operated mail[78] and telephone preference services, which allowed consumers to opt-out of direct marketing.[79] The registries were largely ineffective because they were burdensome—consumers had to either write a letter to register, or pay a fee to be

---

73. Stephen Advokat, *Publication of Bork's Video Rentals Raises Privacy Issue*, CHI. TRIB., Nov. 20, 1987, at 106.

74. *Id.*

75. *See Private Screenings*, ECONOMIST, Mar. 12, 1988, at 31 (describing pending state bans on video rental records release); *Washington News*, UNITED PRESS INT'L, May 10, 1988 (describing congressional efforts to outlaw disclosure of video rental and library records).

76. Ecommerce Topics, Junkbusters, http://www.junkbusters.com/ecommerce.html (last visited Oct. 7, 2006).

77. The Privacy Protection Study Commission ultimately concluded that

> [i]n the private sector, the Commission specifies voluntary compliance . . . if the organizations in an industry have shown themselves willing to cooperate voluntarily. In its mailing list recommendations for example, the Commission specifies that when an organization has a practice of renting, lending, or exchanging the names of its customers, members, or donors for use by others in a direct mail marketing or solicitation, it should inform each of them that it does so and give each an opportunity to veto the practice with respect to his own name. The Commission does not call for legislation to enforce compliance with this recommendation because it has reason to believe the industry is willing to accept these restrictions voluntarily, and there are no legal impediments to stop it from doing so.

PRIVACY PROTECTION STUDY COMMISSION, PERSONAL PRIVACY IN AN INFORMATION SOCIETY 34 (1977); *see also id.* at 150–51 (stating the Commission's belief that voluntary industry reform would successfully address problems of inadequate consumer notice).

78. *Id.* at 141–42, 144–46.

79. CHRIS JAY HOOFNAGLE, ELEC. PRIVACY INFO. CTR., PRIVACY SELF REGULATION: A DECADE OF DISAPPOINTMENT 1 (2005), http://www.epic.org/reports/decadedisappoint.html.

registered by telephone—and consumers were only protected against solicitations from marketers who were DMA members.[80]

In the 1990s, data traders again fended off direct regulation, but this time from the FTC in the area of online commerce. The FTC issued a report to Congress in 1998, concluding that commercial Web sites were not effectively regulating privacy on the Internet, but recommending against legislation because industry leaders had pledged "their commitment to work toward self-regulatory solutions."[81] A year later, the FTC concluded that there had been "important developments" in industry self-regulation, and so again recommended against legislation.[82] The FTC has not revisited the issue, and the seven-year period of industry self-regulation has coincided with the Internet boom, and with it the rapidly expanding possibilities for electronic surveillance, data collection, combining, mining, and direct marketing.[83]

The results of self-regulation have been disappointing from the perspective of information privacy advocates, who have called it a failure and implored Congress and the FTC to disavow data industry self-regulation of privacy.[84] Citing the DMA telephone preference service as an example, critics noted that the DMA registered only 4.8 million consumers in the seventeen years it operated a telephone preference service; the FTC registered 10 million consumers on the first day of the Do-Not-Call list.[85]

Three spectacular private-sector security breaches in 2005—and the legislative responses to them—show that the data industry is still capable of fending off direct government regulation.[86]

In February 2005, ChoicePoint revealed to thousands of Californians that it had sold their personal information, including "names,

---

80. *Id.* at 2.

81. FTC, SELF-REGULATION AND PRIVACY ONLINE: A REPORT TO CONGRESS 1 (1999), http://www.ftc.gov/os/1999/07/privacy99.pdf.

82. *Id.* at 1, 12. These developments included the release of Online Privacy Guidelines by the Online Privacy Alliance, a conglomerate of industry organizations, and the emergence of "seal" programs that monitor privacy policy compliance such as TRUSTe, BBBOnLine, and CPA WebTrust. *Id.* at 8–12.

83. Scholars have described the data industry and invasive technologies in great detail and depth. *See* Froomkin, *supra* note 25, at 1468–1501 (describing and evaluating a variety of "privacy-destroying technologies"); McClurg, *supra* note 8, at 71–87 (explaining the operation of the "consumer profiling industry"); Schwartz, *supra* note 20, at 2060–69 (examining technologies that commercialize personal information).

84. *E.g.*, HOOFNAGLE, *supra* note 79, at 1.

85. *Id.* at 2.

86. For a complete list of data breaches reported since early 2005, see Privacy Rights Clearinghouse, A Chronology of Data Breaches Since the ChoicePoint Incident, http://privacyrights.org/ar/ChronDataBreaches.htm (last visited Oct. 7, 2006).

addresses, Social Security numbers, [and] credit reports," to a ring of identity thieves who had registered fake companies—using previously stolen identities—for the purpose of purchasing personal information.[87] ChoicePoint eventually revealed that it sold the personal data of more than 163,000 people, but refused to specify to the affected consumers exactly what data it had sold.[88]

Shortly thereafter, Bank of America announced that tapes containing the financial data of 1.2 million government employees, including Social Security numbers, were either lost or stolen from an airplane while being shipped to a backup data center.[89]

In March 2005, LexisNexis announced that criminals may have accessed the personal information of 32,000 people, including names, addresses, and Social Security and driver's license numbers, through its subsidiary, Seisint.[90] After completing its security review, LexisNexis increased its estimate, concluding that criminals had accessed the personal information of 310,000 people in fifty-nine separate incidents of security breaches.[91]

The legislative response to these revelations was swift: data security legislation was introduced in at least thirty-one state legislatures and both houses of Congress.[92] Despite this promising start, few of the bills were enacted, and those that were enacted tend to focus spe-

---

87. Bob Sullivan, *Database Giant Gives Access to Fake Firms*, MSNBC.COM, Feb. 14, 2005, http://www.msnbc.msn.com/id/6969799. At the time, California was the only state that required data brokers to reveal security breaches. *Id.*

88. *See* Electronic Privacy Information Center, EPIC ChoicePoint Page, http://www.epic.org/privacy/choicepoint/default.html (last visited Oct. 7, 2006) (describing one victim's inability to procure from ChoicePoint the same personal information that the company had sold to criminals). The FTC charged ChoicePoint with violations of the FCRA and section five of the Fair Trade Commission Act because of false and misleading statements on its Web site regarding its security procedures. Complaint at 7–11, United States v. ChoicePoint Inc., No. 1 06–CV–0198 (N.D. Ga. Jan. 30, 2006), http://www.ftc.gov/os/caselist/choicepoint/0523069complaint.pdf. ChoicePoint settled with the FTC concurrently with the filing of the complaint. Press Release, FTC, ChoicePoint Settles Data Security Breach Charges (Jan. 26, 2006), http://www.ftc.gov/opa/2006/01/choicepoint.htm.

89. CBS News, Bank of America Security Lapse, Feb. 25, 2005, http://www.cbsnews.com/stories/2005/02/25/tech/main676662.shtml.

90. Press Release, Reed Elsevier, LexisNexis Investigates Compromised Customer IDs and Passwords to Seisint US Consumer Data, Mar. 9, 2005, http://www.reed-elsevier.com/index.cfm?articleid=1258.

91. Press Release, LexisNexis, LexisNexis Concludes Review of Data Search Activity, Identifying Additional Instances of Illegal Data Access, Apr. 12, 2005, http://www.lexisnexis.com/about/releases/0789.asp.

92. *See* The State PIRG Consumer Protection Inside Pages, State Breach and Freeze Laws, http://www.pirg.org/consumer/credit/statelaws.htm (last visited Oct. 7, 2006) [hereinafter State PIRG Pages]; *see also infra* notes 97–99 and accompanying text.

cifically on financial and other data found on credit reports, rather than on consumer data more generally.[93]

The state bills generally proposed three ways to "protect" consumers from data security breaches: consumer notification following a security breach, consumer-initiated security freezes on credit reports, and consumer access to credit reports. Notification provisions generally require a data broker to notify an individual when his personal information may have been stolen.[94] Security freezes allow individuals to prevent credit reporting agencies from releasing their credit report without express permission. The security freezes are designed to be consumer friendly, implemented by a written notice or a telephone call to the credit agency.[95] A few bills were proposed allowing consumers to access their data files, obtain a list of everyone who had received the file in the past year, dispute the accuracy of their data, and file a civil action for damages.[96]

Numerous bills dealing with data security were introduced in the United States House and Senate in the spring of 2005. Many of them included notification requirements,[97] security freezes,[98] and access for individuals to their data files.[99] Various bills called for increased FTC oversight and regulation of data brokers[100] and further restrictions on the legal uses of Social Security numbers.[101] Two bills proposed a pri-

---

93. *See, e.g.*, State PIRG Pages, *supra* note 92 (summarizing recently enacted state laws that allow consumers to place holds on their credit reports).

94. *E.g.*, GA. CODE ANN. § 10-1-912 (Supp. 2006) (requiring information brokers to provide notice of any security breach of databases containing personal information to any affected state residents).

95. *E.g.*, N.C. GEN. STAT. § 75-63 (2005) (permitting a consumer to impose a security freeze on his credit report through a written request to a consumer reporting agency); S. 879, 2005 Leg., 421st Sess. (Md. 2005) (same).

96. *E.g.*, S.B. 149, 24th Leg., 1st Sess. §§ 45.48.070, 45.48.190 (Alaska 2005), *available at* http://www.legis.state.ak.us/basis/get_bill_text.asp?hsid=SB0149C&session=24 (providing private right of action against violators of notice and freeze provisions); S.B. 506, 93rd Gen. Assemb., 1st Reg. Sess. § 407.1421 (Mo. 2005), *available at* http://www.senate.mo.gov/05info/billtext/intro/SB506.htm (requiring disclosure of consumer report contents to the consumer upon request, providing the right to dispute inaccurate information, and allowing a civil suit against parties who misuse personal data). One state—Rhode Island—has proposed a statute that gives consumers the right to know what types of personal information a data trader has disclosed to third parties for direct marketing purposes. S.B. 2225, 2006 Leg., Jan. Sess. (R.I. 2006).

97. *E.g.*, S. 1789, 109th Cong. § 421 (2005); S. 1408, 109th Cong. § 3 (2005); H.R. 3140, 109th Cong. §§ 2–3 (2005); S. 1336, 109th Cong. § 7 (2005); S. 751, 109th Cong. § 3 (2005); S. 768, 109th Cong. § 8 (2005); H.R. 1069, 109th Cong. § 3 (2005).

98. *E.g.*, S. 1408 § 4; S. 1336 § 2.

99. *E.g.*, S. 1789 § 301; S. 500, 109th Cong. § 3 (2005).

100. S. 1408 § 2; H.R. 3140 § 2; S. 768 § 3; S. 500 § 3; H.R. 1069 § 7.

101. S. 1408 § 8; H.R. 1745, 109th Cong. (2005); H.R. 1078, 109th Cong. (2005).

vate right of action for individuals.[102] Several bills specified that federal legislation would preempt any state laws governing data brokers,[103] which prompted criticism from privacy advocates that the weaker federal legislation would dismantle the stronger efforts of states like California to protect the privacy of their citizens.[104] After making a quick start, all of the bills were mired down in committees by turf wars and intense lobbying.[105] None became law in 2005, and although some of the bills have emerged from committees, none were passed before the election in 2006.[106]

The state legislation was more successful than the federal, with notification provisions faring best. Before the ChoicePoint scandal, only California required data brokers to notify individuals of security breaches.[107] By mid-2006, thirty-three states had passed laws requiring notification to consumers of data security breaches,[108] but similar legislation failed to pass in thirteen additional states (including a proposal in California to strengthen existing law).[109] By mid-2006, security

---

102. S. 1336 § 10; S. 500 § 4.

103. S. 2169, 109th Cong. § 2 (2005); H.R. 3997, 109th Cong. § 2 (2005); S. 1789 § 303; S. 1408 § 7.

104. Letter from Jeff Chester et al., Executive Director, Center for Digital Democracy, to Sen. Arlen Specter (R-Pa.) and Sen. Patrick Leahy (D-Vt.), Senate Committee on the Judiciary (Nov. 9, 2005), *available at* http://www.epic.org/privacy/choicepoint/datamarker11.09.05.html.

105. Elana Schor, *Data-protection Turf War Pleases Lobbyists*, THE HILL, Aug. 17, 2005, at 11, *available at* http://www.hillnews.com/thehill/export/TheHill/Business/081705_data.html.

106. *E.g.*, H.R. 3997 (approved by Committee on Energy and Commerce on June 2, 2006 and referred to Committee of the Whole House on the State of the Union); S. 1408 (calendared on Dec. 8, 2005); S. 1789 (calendared on Nov. 17, 2005). On June 16, 2006, Senator Hillary Rodham Clinton announced plans to introduce a comprehensive privacy bill, called the Privacy Rights and Oversight for Electronic and Commercial Transactions Act of 2006 (PROTECT Act). Press Release, Senator Hillary Rodham Clinton, Senator Clinton Calls for New Privacy Bill of Rights to Protect Americans' Personal Information (June 16, 2006), http://clinton.senate.gov/news/statements/details.cfm?id=257234&&. The Act would require data brokers to seek consumer permission for data sharing ("opt-in"); create a private cause of action for consumers with tiered statutory-minimum damages ranging from $1,000 to $5,000; give consumers the right to access their own data records, protect their telephone records, freeze their credit reports, and receive notification of security breaches; and create a "privacy czar" at the Office of Management and Budget to oversee privacy practices in the federal government. *Id.*

107. Sullivan, *supra* note 87.

108. These states include Arkansas, Arizona, California, Colorado, Connecticut, Delaware, Florida, Georgia, Hawaii, Idaho, Illinois, Indiana, Kansas, Louisiana, Maine, Minnesota, Montana, Nebraska, Nevada, New Hampshire, New Jersey, New York, North Carolina, North Dakota, Ohio, Oklahoma, Pennsylvania, Rhode Island, Tennessee, Texas, Utah, Washington, and Wisconsin. State PIRG Pages, *supra* note 92.

109. Despite having the strongest data privacy laws in the country, the proposals in California to strengthen existing laws fizzled in 2005, showing that lobbying efforts by data traders remain intense and effective in that state. *See* Insurance Brokers & Agents of the

freezes were enacted in a total of twenty-five states,[110] but were debated and foundered in ten more states (including proposals in California and Texas to strengthen existing laws).[111] Five states—Colorado, Louisiana, New Jersey, North Carolina, and Rhode Island—enacted legislation that creates a private cause of action for consumers when data traders violate their freeze or notice obligations.[112]

In sum, the results of the state and federal legislative efforts of 2005 provide few remedies to privacy-conscious individuals who are injured by unfair or insecure data practices. First, the notification requirements are post facto; they do not help individuals prevent unauthorized access to their data files, and the requirements only apply after a third party gains unauthorized access to data. Thus, notification provides no help for the individual who wants to preemptively control the sale or renting of his data to a third party. Similarly, the security freeze, which allows an individual to control the release of his credit report, does not help the individual who wants to prevent the downstream sale of his nonfinancial personal information—such as transactional or travel data not typically contained in a credit report. Further, the notification and security laws do not allow individuals to access their data files so that they can see what information was released and to whom. Finally, no state passed a law that allows individuals to sue data traders for the injury to their interest in controlling the uses of their personal information.

West, SB 550 Negotiations Resume, http://www.ibawest.com/cgi-bin/beta.asp?SecID=675&ID=8619 (last visited Oct. 7, 2006) (discussing failure of data broker reform legislation to emerge from committee due to financial industry pressure). In 2002, data traders spent more than $20 million in campaign contributions and lobbying expenses to oppose a consumer financial privacy bill in California. Bill Wallace, *$20 Million Tab to Defeat Privacy Bill; Among Priciest Lobbying Efforts in State History*, S.F. CHRON., Sept. 7, 2002, at A1. In 1996, California considered legislation that prohibited data brokers from using or distributing for profit personal information, without that person's written consent. Fenrich, *supra* note 5, at 986 & n.236. However, the bill was killed by a compromise, due to pressure from the credit reporting agency industry lobby. *Id.* at 987–88.

110. These states include California, Colorado, Connecticut, Delaware, Florida, Hawaii, Illinois, Kansas, Kentucky, Louisiana, Maine, Minnesota, Nevada, New Hampshire, New Jersey, New York, North Carolina, Oklahoma, Rhode Island, South Dakota, Texas, Utah, Vermont, Washington, and Wisconsin. State PIRG Pages, *supra* note 92.

111. *Id.*

112. COLO. REV. STAT. ANN. §§ 12-14.3-106.6, -106.7, -107 (West Supp. 2005); LA. REV. STAT. ANN. § 51:3075 (Supp. 2006); N.J. STAT. ANN. §§ 56:11-46(i)(1), -50 (West Supp. 2006); N.C. GEN. STAT. § 75-63 (2005); R.I. GEN. LAWS § 6-48-7 (Supp. 2006) (effective Jan. 1, 2007).

IV. THE EXISTING SCHEME OF PRIVACY TORTS

To suggest that the existing scheme of privacy torts would be an effective tool for addressing the complex problems of personal information abuse is akin to suggesting that one could use a toy drill to fix a nuclear reactor. The tool is clumsy and poorly designed; it does not really fit the parts that are broken; it tends to fall apart when put under pressure; and this particular tool may be running out of batteries just as the situation is getting dire.[113] Manifestly, it is not the right tool for the job. However, in the absence of other solutions, it may be the only tool available, and so it is worth exploring exactly what repair might be done with it.

Privacy torts are typically divided into four categories: intrusion upon seclusion, publication of private facts, publicity that places the plaintiff in a false light, and appropriation of the plaintiff's name or likeness (often known as or conflated with the right of publicity tort).[114] None of these torts comfortably addresses the misuse of personal information, although all have the potential to address certain aspects of data misuse.

A. *Intrusion Upon Seclusion*

The tort of intrusion upon seclusion provides a remedy against someone who "intrudes, physically or otherwise," in a way that would be "highly offensive to a reasonable person," upon the plaintiff's "solitude or seclusion" or "private affairs or concerns."[115] The textbook intrusion tort involves a peeping tom's gaze; a reporter or paparazzo's aggressive or surreptitious pursuit of his targets;[116] or a spy's use of surveillance methods to observe someone in a place where he has a

---

113. *See* Diane L. Zimmerman, *Requiem for a Heavyweight: A Farewell to Warren and Brandeis's Privacy Tort*, 68 CORNELL L. REV. 291, 362–63 (1983) (discussing the inadequacy of common law tort in light of technological developments).

114. *See* RESTATEMENT (SECOND) OF TORTS § 652A (1977) (setting forth the bases for an invasion of privacy cause of action); William L. Prosser, *Privacy*, 48 CAL. L. REV. 383, 389 (1960) (describing the four types of privacy invasion torts).

115. RESTATEMENT (SECOND) OF TORTS § 652B (1977).

116. *See, e.g.*, Dietemann v. Time, Inc., 449 F.2d 245, 247–48 (9th Cir. 1971) (affirming recovery for invasion of privacy when defendant reporter surreptitiously photographed and recorded plaintiff in his home); Sanders v. Am. Broad. Cos., 978 P.2d 67, 69 (Cal. 1999) (holding that defendant reporter's use of a hidden camera in an office environment satisfied the elements of the intrusion tort); Miller v. Nat'l Broad. Co., 232 Cal. Rptr. 668, 670, 678–79 (Cal. Ct. App. 1986) (holding that surviving wife stated an intrusion claim when camera crew followed paramedics into her home and filmed efforts to save her husband); Mitchell v. Balt. Sun Co., 883 A.2d 1008, 1019 (Md. Ct. Spec. App. 2005) (finding a triable issue of fact on an intrusion claim when reporters entered a nursing home room without permission and refused to leave when asked).

reasonable expectation of privacy,[117] such as a home or bathroom stall. The privacy requirement is both subjective and objective; the plaintiff must actually expect privacy, and his expectation of privacy must be objectively reasonable.[118]

As designed, this tort does not address the problems caused by the misuse of information that is already in the possession of the data trader. First, unless the data trader surreptitiously acquired the information (through the use of surveillance or spy ware, for example), the plaintiff cannot show that the trader trespassed or intruded.[119] In *Dwyer v. American Express Co.*,[120] a class of plaintiffs unsuccessfully sued American Express, claiming that its practice of renting lists of card holders' names, organized by purchasing habits, to direct marketers was an intrusion upon their seclusion.[121] This claim foundered on the requirement that the intrusion be unauthorized.[122] The court reasoned that

> [b]y using the American Express card, a cardholder is voluntarily, and necessarily, giving information to defendants that, if analyzed, will reveal a cardholder's spending habits and shopping preferences. We cannot hold that a defendant has

---

117. *See, e.g.*, Schuchart v. La Taberna del Alabardero, Inc., 365 F.3d 33, 36 (D.C. Cir. 2004) (noting that liability for intrusion upon seclusion lies when a defendant "offensively prie[s] into a plaintiff's zone of privacy," including peeping through windows); Doe 2 v. Associated Press, 331 F.3d 417, 422 (4th Cir. 2003) (holding that liability for the tort of intrusion requires actions such as watching or spying in an area in which a person expects to be free from surveillance); Schuler v. McGraw-Hill Cos., 989 F. Supp. 1377, 1390 (D.N.M. 1997) (citing peeping into a private residence as an example of the intrusion tort); Hamberger v. Eastman, 206 A.2d 239, 239–40, 242 (N.H. 1964) (holding that married couple's allegations that landlord installed a listening device in their bedroom stated a claim for intrusion upon seclusion).

118. *See, e.g.*, Shulman v. Group W Prods., Inc. 955 P.2d 469, 490-92 (Cal. 1998) (finding triable issues of fact whether plaintiff had objectively reasonable expectations of privacy in the interior of a rescue helicopter, and in conversations with a medic at the accident scene); Int'l Union v. Garner, 601 F. Supp. 187, 191 (M.D. Tenn. 1985) (finding no reasonable expectation of privacy in plaintiff's attendance at a union meeting); RESTATEMENT (SECOND) OF TORTS § 652B cmt. c (noting that the defendant is liable only for intruding into a "private place" or a "private seclusion that the plaintiff has thrown about his person or affairs").

119. *See Doe 2*, 331 F.3d at 422 (holding that the tort of intrusion requires actions such as "watching, spying, prying, besetting, [or] overhearing" (alteration in original) (internal quotation marks omitted)); Wolf v. Regardie, 553 A.2d 1213, 1217–18 (D.C. 1989) (listing examples of intrusion, including spying, reading another's mail, eavesdropping, and trespassing); Humphers v. First Interstate Bank, 696 P.2d 527, 532–33 (Or. 1985) (finding no intrusion when a doctor revealed information on a confidential adoption form in his possession because he did not "pry into any personal facts that he did not [already] know").

120. 652 N.E.2d 1351 (Ill. App. Ct. 1995).

121. *Id.* at 1352–54.

122. *Id.* at 1354.

> committed an unauthorized intrusion by compiling the information voluntarily given to it and then renting its compilation.[123]

Second, as *Dwyer* suggests, it may be difficult for an individual to prove that she has a subjective or objective expectation of privacy in information such as her name, birth date, address, and telephone number, or records of clickstream data, travel itineraries, grocery purchases and other transactional data, especially if she has willingly surrendered that information in exchange for some proffered advantage.[124] Most individuals routinely provide identifying information (such as name, address, telephone number, and birth date) when asked—online or offline—suggesting that they do not consider this information private in the same way that they might consider their medical data private. Because travel and offline purchases take place in public, a plaintiff would struggle to establish both subjective and objective expectations of privacy in this information. A plaintiff could probably establish a subjective expectation of privacy in clickstream data, especially if she has accessed the Internet from her home, but sustaining a reasonable expectation argument would be more difficult, as few people are so naïve anymore as to expect anonymity on the Web.

Even people who fiercely guard their identities will be hard pressed to establish a reasonable expectation of privacy in their names. During a *Terry* stop,[125] for example, a police officer can demand a name from the suspect without offending the Fourth Amendment,[126] suggesting that there is little, if any, reasonable expectation of privacy in one's name.[127]

If, on the other hand, a plaintiff can argue that the data trader has used her name, address, and birth date in combination with other more sensitive information, she might be able to show an expectation of privacy. In *Weld v. CVS Pharmacy, Inc.*,[128] a Massachusetts superior court refused to grant summary judgment to a defendant drugstore when the plaintiffs alleged that the defendant's direct marketing

---

123. *Id.*

124. *See id.* (emphasizing that plaintiffs voluntarily gave defendant access to the spending habit data at issue in the lawsuit).

125. *See* Terry v. Ohio, 392 U.S. 1 (1968) (holding that a police officer may constitutionally stop and frisk a suspect upon reasonable suspicion that the suspect poses a safety threat).

126. Hiibel v. Sixth Jud. Dist. Ct., 542 U.S. 177, 185 (2004).

127. *See id.* at 191 (opining that "[o]ne's identity is, by definition, unique; yet it is, in another sense, a universal characteristic").

128. No. Civ. A. 98-0897F, 1999 WL 494114 (Mass. Super. Ct. June 29, 1999).

scheme invaded their privacy.[129] Without consent, CVS Pharmacy, Inc. (CVS) "mined" its customer prescription records for the purpose of sending its customers mailings targeted to their specific medical conditions, based on prescriptions they had previously filled.[130] CVS then gave the names, addresses, and birth dates—but no other sensitive medical information—to a direct marketer who prepared the mailings. CVS received a fee for each mailing from one of various drug manufacturers.[131] CVS argued that the Massachusetts privacy statute was not violated by the disclosure of names, addresses, and birth dates.[132] The court rejected this approach, noting that the plaintiffs had complained about the use of that information "in conjunction with the systematic searching of customer prescription records."[133] Consent issues aside, the *Weld* court's approach suggests that a more expansive view of private information—one that incorporates the ways that information is mined or analyzed—could make this tort viable for protecting information privacy.

B. Public Disclosure of a Private Fact

The public disclosure tort provides a remedy against someone who publicizes private information about the plaintiff if the information is "not of legitimate concern to the public" and its publication "would be highly offensive to a reasonable person."[134] The tort compensates the plaintiff for the mental distress—shame, humiliation, and anger—caused by the public display of intimate and embarrassing information.[135] The classic example of a public disclosure tort is the small town merchant who posts in his shop window, visible to all who pass by, a true statement that the plaintiff owes him money and has not repaid him.[136] In the past three decades, this tort has been deci-

---

129. *Id.* at *1.
130. *Id.*
131. *Id.* at *1–2.
132. *Id.* at *3.
133. *Id.* at *4.
134. RESTATEMENT (SECOND) OF TORTS § 652D (1977).
135. *See* Talley v. Farrell, 156 F. Supp. 2d 534, 544 (D. Md. 2001) (stating that the defendant's disclosure must be sufficiently offensive to carry "overtones of mental distress" for plaintiff to recover for unreasonable publicity); Taylor v. NationsBank N.A., 738 A.2d 893, 897 (Md. Ct. Spec. App. 1999) (same); GEORGE B. TRUBOW, PRIVACY LAW & PRACTICE ¶ 1.05 (1991) (stating that recovery is intended to compensate for mental distress caused by injury to plaintiff's dignity).
136. Brents v. Morgan, 299 S.W. 967, 968 (Ky. 1927); Prosser, *supra* note 114, at 392 (citing *Brents* as the first application of the "public disclosure of private facts" tort); *see also* Fernandez v. United Acceptance Corp., 610 P.2d 461, 464 (Ariz. Ct. App. 1980) (holding that plaintiffs' recovery for invasion of privacy was proper when defendant called plaintiffs' neighbors and employers in attempt to collect plaintiffs' debt); Trammell v. Citizens News

mated by First Amendment limitations on the definition of what is private and on what information is of legitimate concern to the public.[137] Hypothetically, however, these First Amendment limitations would not apply to individual consumer transactions of an embarrassing sort when the individual is not a public figure. Thus, for example, an individual would probably avoid the newsworthiness problem if he sued a data trader who had widely sold the true information that the plaintiff habitually used his American Express Card to purchase racy underwear over the Internet at 3:00 A.M.

Plaintiffs who want to use (the remnants of) this tort to redress the misuse of personal information will face a significant hurdle in proving that data traders have publicized personal information. Data traders typically sell information to other companies (or even government agencies), but do not broadcast their information, in the sense of releasing it for use by the general public. This type of sale is not clearly included in the *Restatement*'s definition of publicity, which requires that the information be communicated to "the public at large."[138] Thus, for example, the disclosure of embarrassing information to a small group of the plaintiff's coworkers,[139] or to a few rela-

---

Co., 148 S.W.2d 708, 709–10 (Ky. 1941) (holding that newspaper's publication of plaintiff's debt was a public disclosure of private facts sufficient to create a cause of action in tort against the newspaper); Biederman's of Springfield, Inc. v. Wright, 322 S.W.2d 892, 893, 898 (Mo. 1959) (holding that plaintiff stated a claim for invasion of privacy when a creditor loudly demanded payment of plaintiff's debts at plaintiff's place of employment).

137. *See, e.g.*, Cox Broad. Corp. v. Cohn, 420 U.S. 469, 496–97 (1975) (invalidating on First Amendment grounds a state statute that established liability for the broadcast of a rape victim's name, when the broadcaster obtained the name from public records). After *Cox*, information contained in a public record that is subject to disclosure under a freedom of information or sunshine law generally is not considered private. Furthermore, voluntary and involuntary public figures generally cannot sue for the publication of truthful information, even if the information published exceeds the scope of the figure's notoriety. *E.g.*, Capra v. Thoroughbred Racing Ass'n of N. Am., Inc., 787 F.2d 463, 464–65 (9th Cir. 1986) (per curiam) (finding that participants in the federal witness protection program must prove publication of their real names was not newsworthy for their claim to survive); Virgil v. Time, Inc., 527 F.2d 1122, 1128–29 (9th Cir. 1975) (discussing the exemption from tort liability for publication of newsworthy personal information). *See generally* Zimmerman, *supra* note 113, 341–62 (discussing the constitutional and practical problems with the private facts tort).

138. RESTATEMENT (SECOND) OF TORTS § 652D cmt. a. The *Restatement* explicitly distinguishes the publicity requirement from "publication," as used in the defamation context, which requires disclosure only to a third party. *Id.*

139. Dancy v. Fina Oil & Chem. Co., 3 F. Supp. 2d 737, 738, 740 (E.D. Tex. 1997) (finding that employer's publication to supervisors, union heads, and other employees, of a list of employees with excessive absences did not satisfy the publicity element of the invasion of privacy tort).

tives and an employer,[140] is not considered publicity in most jurisdictions. The courts that have deviated from the *Restatement* have looked for a "special relationship . . . between the plaintiff and the 'public' to whom the information has been disclosed,"[141] such that exposure of those facts to that public—even if constituted of only one person—would embarrass the plaintiff.[142] In the underwear hypothetical, the information about the underwear purchases is most likely being made available to vendors of similar or related merchandise, and thus is not likely to embarrass the plaintiff; rather, it might facilitate his predilections. On the other hand, the publicity requirement might be met if the defendant's security had been so lax that the information had effectively been publicized.

Assuming, however, that a plaintiff could top the publicity hurdle, there is some promise in using the public disclosure tort to redress the sale of information considered embarrassing, and thus highly offensive, if disclosed. While the publication of personal information such as names, birthdates, addresses, and telephone numbers generally fails the highly offensive test,[143] it is more likely that the publication of travel and transactional data could be considered highly offensive, especially—as in digital dossiers—when the reports are comprehensive (listing every trip or transaction in the past several years), or the items purchased (underwear, books, medicines) are

---

140. *See* Vogel v. W.T. Grant Co., 327 A.2d 133, 134, 137 (Pa. 1974) (holding that a creditor's communication of debt details to the employers and relatives of debtors was not sufficient publicity to satisfy the requirement).

141. McSurely v. McClellan, 753 F.2d 88, 112 (D.C. Cir. 1985).

142. Beaumont v. Brown, 257 N.W.2d 522, 531–32 (Mich. 1977) (holding that the publicity element is satisfied by publication of private information to "a public whose knowledge of those facts would be embarrassing to the plaintiff"), *partially overruled on other grounds by* Bradley v. Saranac Cmty. Sch. Bd. of Educ., 565 N.W.2d 650 (Mich. 1997).

143. *See* Cox Broad. Corp. v. Cohn, 420 U.S. 469, 495 (1975) (emphasizing that rape victim's name was a matter of public record in finding no invasion of privacy when a newspaper published the victim's name); Meetze v. Associated Press, 95 S.E.2d 606, 610 (S.C. 1956) (finding no invasion of privacy in newspaper's publication of information that a twelve-year-old girl gave birth to a healthy child when information was a matter of public record); RESTATEMENT (SECOND) OF TORTS § 652D (noting that the tort of invasion of privacy includes the publicizing of a matter that "would be highly offensive to a reasonable person").

There is some indication that the publication of Social Security numbers would be treated as "highly offensive." *See, e.g.*, Progressive Animal Welfare Soc'y v. Univ. of Wash., 884 P.2d 592, 598 (Wash. 1994) (stating in dicta that "disclosure of a public employee's [S]ocial [S]ecurity number would be highly offensive to a reasonable person"). *See generally* Lora M. Jennings, Comment, *Paying the Price for Privacy: Using the Private Facts Tort to Control Social Security Number Dissemination and the Risk of Identity Theft*, 43 WASHBURN L.J. 725 (2004) (arguing that the publication of Social Security numbers should be considered highly offensive and remediable under the publication of private facts tort).

more intimately revealing.[144] Despite this possibility, plaintiffs may struggle to show that the publication of information is highly offensive in our full-disclosure society. When people reveal their most embarrassing secrets on *Maury*, *The Oprah Winfrey Show*, pod casts, and blogs, or consent to cameras following their most intimate choices and times of fear and stress, it is difficult to see how the revelation of one's purchasing habits could cause a credible emotional injury.

C. False Light

The tort of false light provides a remedy against someone who publicizes a matter concerning the plaintiff and in so doing portrays him in a way that is both false and objectionable.[145] The interest protected is the plaintiff's dignity, and his right to be portrayed as he is and to avoid being portrayed in an offensively false manner.[146] The typical false light case involves a plaintiff whose photograph, taken in one context, is later published in a different context that creates a false and offensive suggestion.[147]

As with the private facts tort, plaintiffs who want to use false light to redress the misuse of personal information will face a significant (if not insurmountable) hurdle in proving that data traders have publicized personal information.[148] Assuming, however, that the sale of in-

---

144. The *Restatement* leaves open the possibility that publication based on careful or thorough—rather than casual—observation might qualify as highly offensive. RESTATEMENT (SECOND) OF TORTS § 652D cmt. on cl. a (stating that casual notice of one's activities is to be expected; liability only attaches when a reasonable individual would be "seriously aggrieved" by the publicity).

145. *Id.* § 652E. It is yet undecided whether the defendant must act with reckless disregard for the truth, or whether he can be liable for mere negligence. *Id.*

146. *Id.* § 652E cmt. b. False light is distinct from defamation, which protects the plaintiff's interest in maintaining a good reputation. False light thus protects a personal interest—what one thinks of oneself, while defamation protects a relational interest—what others think of one. PROSSER & KEETON ON THE LAW OF TORTS § 117 (5th ed. 1984).

147. *See, e.g.*, Braun v. Flynt, 726 F.2d 245, 247, 252, 254 (5th Cir. 1984) (holding that publication of plaintiff with "Ralph, the Diving Pig" among pornographic photographs in magazine created actionable disparaging suggestion about plaintiff's character); Leverton v. Curtis Publ'g Co., 192 F.2d 974, 977–78 (3d Cir. 1951) (affirming jury award for invasion of privacy when a publisher used a photograph of a law-abiding, near-victim of an accident in an unrelated article on the carelessness of pedestrians); Gill v. Curtis Publ'g Co., 239 P.2d 630, 635 (Cal. 1952) (holding that a photograph of a couple captioned as two people who experienced "love at first sight" connected with an article saying such love is based on 100% sex is sufficient to state a claim for invasion of privacy).

148. RESTATEMENT (SECOND) OF TORTS § 652E cmt. a (equating the publicity element of the false light tort with the publicity element of the private facts tort); *see also* Veilleux v. Nat'l Broad. Co., 206 F.3d 92, 134 (1st Cir. 2000) (applying Maine law, which follows the *Restatement* definition of false light); White v. Fraternal Order of Police, 909 F.2d 512, 522 (D.C. Cir. 1990) (citing elements of *Restatement* definition of false light tort); West v. Media

formation to other data traders could be considered publicity, this action could be a useful means of addressing the sale of false information that portrays the plaintiff in an objectionable way. The *Restatement* explicitly excludes from this tort false information about insignificant details, such as a person's correct address, except under "special circumstances."[149] However, if a data trader transfers sufficiently significant information, such as an inaccurate misdemeanor conviction, the tort might provide a remedy. Of course, this tort requires that the resulting portrayal of the plaintiff be false, and so it entirely misses the misuse of truthful information. In many cases of information abuse, the problem is that the information "publicized" is all too accurate, allowing others to steal or gain unwanted access to the plaintiff's identity.

D. Appropriation and the Right of Publicity

The appropriation tort provides a remedy against a defendant who appropriates the plaintiff's name or likeness without the plaintiff's permission and uses it for the defendant's own benefit, usually, but not necessarily, in a commercial context.[150] This tort protects the plaintiff's interest in controlling the use of her identity and compensates the mental distress or commercial loss of a person whose name or image is used without permission.[151] The *Restatement* indicates that the tort does not protect a person's name as such, but rather protects the "values or benefits" of that name, such as the individual's "prestige, social or commercial standing."[152] Appropriation, which was the first privacy tort recognized in this country,[153] is often conflated with

---

Gen. Convergence, Inc., 53 S.W.3d 640, 643–45 (Tenn. 2001) (adopting the *Restatement* definition of the tort of false light invasion of privacy, including the publicity element).

149. RESTATEMENT (SECOND) OF TORTS § 652E cmt. c.

150. *Id.* § 652C cmt. b.

151. Taylor v. City of Demopolis, No. Civ. A. 04-758-BH-B, 2005 WL 3320735, at *12–13 (S.D. Ala. Dec. 6, 2005) (noting that appropriation tort compensates "'damage to human dignity'" (quoting Allison v. Vintage Sports Plaques, 136 F.3d 1443, 1446 (11th Cir. 1998)); Fairfield v. Am. Photocopy Equip. Co., 291 P.2d 194, 197–98 (Cal. Dist. Ct. App. 1955) (holding that attorney could recover damages for injury to his peace of mind and feelings when company used his name in advertisement without permission)); J. THOMAS MCCARTHY, 1 THE RIGHTS OF PUBLICITY AND PRIVACY § 1:26 (2d ed. 2006) (reviewing the emergence of the appropriation tort in protection of a commercial interest in one's identity).

152. RESTATEMENT (SECOND) OF TORTS § 652C cmt. c.

153. *See* Pavesich v. New Eng. Life Ins. Co., 50 S.E. 68, 68–69, 71 (Ga. 1905) (acknowledging for the first time that a common law right of privacy had been violated by the unauthorized commercial use of a person's identity); Prosser, *supra* note 114, at 386 (stating that *Pavesich* was the leading decision holding that tort law recognized infringement upon the right to privacy).

the right of publicity,[154] which more specifically protects a property interest in identity, awarding damages based on the commercial value of that identity.[155] The two causes of action address the same behavior by the defendant (the unauthorized use of identity to benefit the defendant), but award damages based on different theories.[156] Right of publicity plaintiffs tend to be celebrities, while appropriation plaintiffs tend to be those whose identities have less readily quantifiable commercial value.[157]

The typical appropriation case involves a non-famous plaintiff whose name or photograph is used without permission in an advertisement.[158] The issues in these cases often focus on whether the defen-

---

154. Professor McCarthy, for example, defines the right of publicity as the "inherent right of every human being to control the commercial use of his or her identity," which is sufficiently broad to subsume the appropriation tort. MCCARTHY, *supra* note 151, § 1:3; *see also* Harold R. Gordon, *Right of Property in Name, Likeness, Personality and History*, 55 NW. U. L. REV. 553, 555 (1960) (defining right of publicity as "the right to be free from commercial exploitation" (emphasis omitted)). Professor McCarthy views the right as a hybrid of privacy (addressing the mental distress of seeing one's name or image used without permission), unfair competition (prohibiting the use without permission of the commercial value of a person's identity for the purposes of trade), and intellectual property (protecting a property right in the commercial value of one's identity). MCCARTHY, *supra* note 151, §§ 1:6, 1:7; RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 47 (1995) (describing the use of a person's identity "for purposes of trade"); *see also* LIBEL DEF. RES. CTR., INC., LDRC 50-STATE SURVEY: MEDIA PRIVACY AND RELATED LAW, 2002–2003, at 1520 (combining misappropriation and right of publicity in same row of issue table). It is generally accepted, however, that the right of publicity grew out of the tort of appropriation. *See* Roberta Rosenthal Kwall, *Is Independence Day Dawning for the Right of Publicity?*, 17 U.C. DAVIS L. REV. 191, 193 (1983) (stating that the right of publicity sprang from privacy doctrine and noting the historical connection between the right of publicity and the appropriation tort); RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 46 cmt. b (1995) (stating that the right of publicity has its historical roots in application of the appropriation tort in commercial circumstances).

155. *See, e.g.*, Parks v. LaFace Records, 329 F.3d 437, 460 (6th Cir. 2003) (stating that the right of publicity tort gives a celebrity the right to defend an "economic interest in his or her name"); Herman Miller, Inc. v. Palazzetti Imps. & Exps., Inc., 270 F.3d 298, 325 (6th Cir. 2001) (stating that the right of publicity protects a commercial interest and is a property right); Landham v. Lewis Galoob Toys, Inc., 227 F.3d 619, 624 (6th Cir. 2000) (stating that the right of publicity preserves the right of a person to use his identity commercially).

156. *See* MCCARTHY, *supra* note 151, § 1:7 (distinguishing pecuniary and psychological damages). Depending on the circumstances, the misuse of personal information might fit either or both theories: the injury to dignity caused by the unauthorized use of personal information or by the existence of a digital doppelganger compiled without permission (appropriation); the injury to pocketbook caused by identity theft (publicity).

157. *See id.* (noting that the right of publicity developed to address famous plaintiffs' claims).

158. *See, e.g.*, Fanelle v. LoJack Corp., 79 F. Supp. 2d 558, 560, 564 (E.D. Pa. 2000) (holding that unauthorized use of photograph of individual charged with car theft in an anti-theft advertisement stated a claim of appropriation); Pavesich v. New Eng. Life Ins. Co., 50 S.E. 68, 79 (Ga. 1905) (holding that unauthorized use of photograph of plaintiff in advertisement for life insurance was an invasion of privacy); Harbin v. Jennings, 734 So. 2d 269,

dant's use was commercial—although the *Restatement* specifically notes that the use need not be commercial, and cases have been successfully pursued in noncommercial contexts.[159] In an effort to protect the freedom of the press, the bar for determining whether the defendant's use was commercial has been set high. The use must be an explicit "solicitation for patronage."[160] If the use involves matters of even remotely public interest and the plaintiff's identity is reasonably related to the matter, the use is considered newsworthy, protected by the First Amendment, and not commercial.[161] In practice, the newsworthiness standard is a significant obstacle for plaintiffs bringing appropriation claims.[162]

The classic publicity case involves the use of a celebrity's identity without permission as an endorsement for a product. The issues in such cases often revolve around identification—whether the plaintiff is sufficiently identifiable from the defendant's use. In most jurisdictions, the right of publicity is not strictly limited to the defendant's use of the plaintiff's "name or likeness."[163] Most common law states interpret the traditional phrases "name or likeness" to include any aspect of the plaintiff's persona, including vocal style, body movement, costume, makeup, setting, nickname, or a combination of any of these. Thus, for example, a robotic simulacrum of Vanna White was suffi-

---

272 (Miss. Ct. App. 1999) (noting that unauthorized use of a photograph in picture frames displayed to the public was a "textbook example" of appropriation); Faber v. Condecor, Inc., 477 A.2d 1289, 1294–95 (N.J. Super. Ct. App. Div. 1984) (affirming jury award for defendant's unauthorized use of plaintiffs' photograph in picture frame display); Flake v. Greensboro News Co., 195 S.E. 55, 64 (N.C. 1938) (holding that the use of photograph in an advertisement without the subject's permission is an actionable invasion of privacy).

159. *See, e.g.*, Steding v. Battistoni, 208 A.2d 559, 562 (Conn. Cir. Ct. 1964) (stating that using the name of another to pursue legal action was appropriation); Hinish v. Meier & Frank Co., 113 P.2d 438, 439, 448 (Or. 1941) (holding that plaintiff stated an appropriation claim against defendant who signed plaintiff's name on a telegram to the governor).

160. Lahiri v. Daily Mirror, Inc., 295 N.Y.S. 382, 386 (Sup. Ct. 1937).

161. *See, e.g.*, Arrington v. N.Y. Times Co., 434 N.E.2d 1319, 1320, 1322–23 (N.Y. 1982) (finding no appropriation when newspaper published plaintiff's photograph next to an article about the "black middle class" because the photograph was related to an article of public interest); *Lahiri*, 295 N.Y.S. at 389–90 (finding no appropriation when newspaper published plaintiff's photograph in article about a "famous rope trick" because it related to a matter of legitimate news interest (internal quotation marks omitted)).

162. *See* Claire E. Gorman, Comment, *Publicity and Privacy Rights: Evening Out the Playing Field for Celebrities and Private Citizens in the Modern Game of Mass Media*, 53 DEPAUL L. REV. 1247, 1263–68 (2004) (describing the First Amendment obstacles that plaintiffs face when asserting right of privacy claims).

163. *See* White v. Samsung Elecs. Am., Inc. 971 F.2d 1395, 1397–99 (9th Cir. 1992) (rejecting lower court's limitation of appropriation tort to plaintiff's "name or likeness"). However, some states with publicity statutes narrowly limit these terms. *E.g.*, N.Y. CIV. RTS. § 51 (McKinney 1992 & Supp. 2006) (limiting recovery to appropriation of plaintiff's "name, portrait, picture or voice").

ciently identifiable as White—through dress, mannerisms, hairstyle, and context—to be actionable.[164]

Of all the branches of privacy torts, commentators have identified the appropriation/right of publicity torts in their broadest forms as the most promising for addressing the misuse of personal information, for two reasons. First, understood broadly, the rights protected by these torts are infringed whenever a defendant, without permission, makes a commercial use of the plaintiff's identity that either causes the plaintiff mental distress or damages the value of the plaintiff's identity.[165] Thus, the torts theoretically redress nonconsensual uses of personal information—such as the combining, profiling, and mining of information that causes mental distress, or the sale of information that causes the fear of identity theft or actual identity theft.

Second, the breadth with which courts have treated identity also seems promising. Data traders deal quite specifically in information that identifies a person, and the value of the information is based on the accuracy and completeness with which the person is identified. The broad definition of personality means that these torts could extend to identifying information—such as addresses, telephone numbers, birthdates, Social Security numbers, travel and transactional data—because a combination of these items (or indeed some of them individually) would suffice to accurately identify the plaintiff.

In practice, however, data traders have never successfully been sued using these privacy torts. One limitation on their use is that the torts presume that the defendant is using the plaintiff's identity for his own advantage. Thus, the torts miss situations in which data traders misuse personal information through negligent handling or the accidental release of personal information, which are typically errors, not practices that advantage the defendant. Even the failure to rectify incorrect information is arguably not to the data trader's advantage.

More importantly, data trading does not easily mesh with the tort's paradigm, which involves the use of the plaintiff's name or likeness in an advertisement. Courts may struggle with the analogy to data brokers, who trade in lists or databases of personal information. Two cases all but killed the prospects of using this tort to address the

---

164. *White*, 971 F.2d at 1396, 1399; *see also* Abdul-Jabbar v. Gen. Motors Corp., 85 F.3d 407, 414–15 (9th Cir. 1996) (finding "name and likeness" not limited to present use and allowing an athlete to pursue an action for the appropriation of his former name); Waits v. Frito-Lay, Inc., 978 F.2d 1093, 1098, 1100, 1112 (9th Cir. 1992) (upholding a verdict against a snack manufacturer for appropriating the voice of well-known singer Tom Waits in a radio commercial).

165. *See, e.g.*, MCCARTHY, *supra* note 151, at v (commenting that the legal right of publicity protects an individual's "inherent" ownership of his identity).

misuse of personal information. In the much-maligned *Shibley v. Time, Inc.*,[166] an Ohio court held that the sale by *Time Magazine* of subscription lists to direct marketers was not an actionable appropriation of the plaintiffs' names. The reasoning in *Shibley* was based on two authorities: an Ohio statute authorizing the sale of car registration records,[167] and a federal case[168] upholding a New York statute that authorized the state to sell its lists of registered car owners to direct marketers.[169] The court apparently reasoned that the legal sale of such records indicated that individuals did not have a protected privacy interest in their identifying information.[170] The *Dwyer* court, relying on *Shibley*, also dismissed an appropriation claim, finding that the plaintiffs had failed to show an appropriation because "a single, random cardholder's name has little or no intrinsic value."[171] Rather, the value attached to the name derived from the aggregation and analysis of the data conducted by American Express.[172]

Two more recent cases show that the appropriation tort may yet accommodate information privacy claims. In 2003, the Supreme Court of New Hampshire dismissed an appropriation claim against a private investigator who sold information about a woman to her stalker who later killed her.[173] The court reasoned that the investigator sold the information "for the value of the information itself, not to take advantage of the person's reputation or prestige."[174] This line of reasoning suggests that the observe theory might succeed: a data trader who compiles and sells lists of information not for the value of the information itself, but *precisely because* it hopes to trade on the individuals' "social or commercial standing"[175]—their spending habits,

166. 341 N.E.2d 337 (Ohio Ct. App. 1975).

167. *Id.* at 339.

168. Lamont v. Comm'r of Motor Vehicles, 269 F. Supp. 880 (S.D.N.Y. 1967).

169. *Shibley*, 341 N.E.2d at 339–40. The Ohio and New York statutes have since been superseded by the Driver's Privacy Protection Act of 1994 (DPPA), which prevents states from disclosing a driver's personal information without his consent. 18 U.S.C. §§ 2721–2725 (2000); *see also* Pub. L. No. 106-69, § 350g, 113 Stat. 1025 (1999) (including New York and Ohio as states where the DPPA applies). The Supreme Court upheld the constitutionality of the DPPA in *Reno v. Condon*, 528 U.S. 141 (2000).

170. *See Shibley*, 341 N.E.2d at 339–40. This line of reasoning invalidates the very interest protected by the appropriation tort—the right to control the use of one's identity.

171. Dwyer v. Am. Express Co., 652 N.E.2d 1351, 1356 (Ill. App. Ct. 1995).

172. *Id.* Others have noted the difficulty of quantifying the value of one name or one set of personal data. Generally, data is traded in batches, and so is more valuable in the aggregate than in individual units. McClurg, *supra* note 8, at 118. For an analysis of the failures of the personal information market, see Schwartz, *supra* note 20, at 2076–84.

173. Remsburg v. Docusearch, Inc., 816 A.2d 1001, 1010 (N.H. 2003).

174. *Id.*

175. *Id.*

preferences, interests, or creditworthiness—would be liable for appropriation, at least in the state of New Hampshire.

The *Weld* court also took an expansive view of the appropriation tort, noting that the tort is not strictly limited to commercial or advertising uses, but that it also applies when the defendant uses the plaintiff's name "'for his own purposes and benefit . . . even though the benefit . . . is not a pecuniary one.'"[176] Based on the factual scenario in that case—CVS used the plaintiffs' private information for financial gain—the plaintiffs had alleged a violation of the appropriation tort. It is unlikely, however, that *Weld* will generate positive precedent, as the common law tort of appropriation is probably preempted by statute in Massachusetts.[177]

Despite some promising dicta, the fact remains that plaintiffs using privacy tort theories have never yet held data traders accountable for misusing the personal information of data subjects. The torts are possibly useful if it can be shown, as in *Weld*, that using a name as part of a process invades a person's privacy, or, as noted in *Remsburg*, that the data trader has sold the plaintiff's identifying information to profit from her social standing or prestige. In general, however, the torts as formulated by Prosser are not a comfortable fit with the trading of personal information. The major obstacles are that first, the definition of "private" is too narrow to cover much of the personal information in data files; second, the publicity requirement is not clearly met by commercial transactions; third, the highly offensive requirement may be difficult to meet in today's tell-all world; and fourth, the sale of personal information does not easily mesh with the paradigm for the appropriation tort. Tort law in its current form has failed to evolve adequately and sufficiently to address information abuse; the misuses have outpaced the current system. It thus remains an unlikely option for individuals searching for information privacy remedies, unless a new tort that better fits the harms of information misuse evolves.

V. WHAT IS TO BE DONE?

A comparative history of products liability provides a useful analogy, as well as the basis of this Article's argument, that tort law is a time-honored vehicle for facilitating solutions to emerging harms. The European model is creationist: a central authority enacts univer-

176. Weld v. CVS Pharmacy, Inc., No. Civ. A. 98-0897F, 1999 WL 494114, at *6 (Mass. Super. Ct. June 29, 1999) (quoting RESTATEMENT (SECOND) OF TORTS § 652C cmt. b (1977)).

177. *Id.*

sal model legislation, such as the Liability for Defective Products Directive,[178] that results in the gradual harmonization of products liability laws in the member states of the European Community.[179] By contrast, the American model, which relies on individual plaintiffs and injuries, is Darwinian. After the British courts failed to act in products liability cases, state courts in this country experimented with various evolving theories of liability, including exceptions to the rule of privity, and extensions to the categories of who could sue whom, for what types of injuries, and from what types of products.[180] Eventually, the common law coalesced around the principle of strict liability,[181] which has since been adopted, modified, or left alone by state legislatures.

Remarkably, we are following neither the creationist nor the Darwinian model in addressing the injuries caused by the misuse of personal information.[182] However, because it is now clear that industry lobbying has succeeded while self-regulation has failed, and that legislatures have either failed to act or provided solutions that inadequately address the injuries, individuals must—indeed, should—look to the judiciary to help resolve the misuse of personal information.[183]

---

178. Council Directive 85/374, 1985 O.J. (L 210) 29 (EC).

179. *See* Sandra N. Hurd & Frances E. Zollers, *Desperately Seeking Harmony: The European Community's Search for Uniformity in Product Liability Law*, 30 AM. BUS. L.J. 35 (1992); Sandra N. Hurd & Frances E. Zollers, *Product Liability in the European Community: Implications for United States Business*, 31 AM. BUS. L.J. 245 (1993).

180. *See* RICHARD A. EPSTEIN, MODERN PRODUCTS LIABILITY LAW 9–24 (1980) (discussing the American judiciary's departure from British common law rule of privity).

181. *See, e.g.*, William L. Prosser, *The Assault upon the Citadel (Strict Liability to the Consumer)*, 69 YALE L.J. 1099, 1103–10 (1960) (discussing the unmooring of privity of contract from torts involving food and drink law and the imposition of strict liability for claims); William L. Prosser, *The Fall of the Citadel (Strict Liability to the Consumer)*, 50 MINN. L. REV. 791, 794–97 (1966) (documenting the spread of strict liability to other areas of law).

182. "The United States may be unique in endorsing self-regulation without legal sanctions to incentivize or enforce it; it is hard to believe that the strategy is anything more than a political device to avoid regulation." Froomkin, *supra* note 25, at 1527 (footnote omitted).

183. Public choice theory predicts the failure of Congress to pass legislation protecting consumers against information abuse: as a narrow and well-funded interest group, data traders have attempted to block legislation that would benefit a widely dispersed and not well-organized group. *Cf.* DANIEL A. FARBER & PHILIP P. FRICKEY, LAW & PUBLIC CHOICE: A CRITICAL INTRODUCTION 33 (1991) (depicting the role of special interest groups in influencing legislative behavior). Judicial creativity is arguably a valid response in such circumstances, particularly when interest groups have distorted the legislative process and tort wrongs are left unremedied. *See* Fenrich, *supra* note 5, at 994–95 (advocating that courts should take an active role in extending tort law to cover cases of information abuse); Edmund Ursin, *Judicial Creativity and Tort Law*, 49 GEO. WASH. L. REV. 229, 245–50 (1981) (arguing that the judiciary is better positioned to create tort reform than legislators who are beholden to special interest groups); *see also* Daniel A. Farber & Philip P. Frickey, *In the Shadow of the Legislature: The Common Law in the Age of the New Public Law*, 89 MICH. L. REV.

It is again time to propose a tort for the misuse of personal information.[184] The new tort will borrow from existing areas of law—the four privacy torts and existing privacy statutes—but will be tailored to address the specifics of information abuse. Seen in the context of existing privacy torts and statutes, the tort is not a radical departure from the existing scheme, but more of a gap-filler or a cautious expansion, as it addresses injuries that implicate core privacy interests but currently have no remedy. Like the appropriation tort, the new tort remedies the harm to an individual caused by his loss of control over his identity when a data trader uses it without his permission. Like the Privacy Act, the new tort uses the principles of Fair Information Practices—notice, choice, access, and security[185]—as the minimum standard for acceptable data management. The tort charts new ground in expanding the definition of what is considered private, in targeting commercial uses of data, and in transferring the principles of Fair Information Practices from the public sector to the private sector. This is what the tort would look like:

- One who collects, stores, analyzes, or trades in personal information is liable to the subject of that information for the failure to use Fair Information Practices.
- The tort would apply to any private entity that collects, stores, analyzes, or trades in personal information.
- Personal information would include any information that is linked with an individual.
- The tort would impose on data traders a duty to use Fair Information Practices (based on the principles of notice, choice, access, and security).
- The tort would protect the individual's privacy interests in choice and control—choice about who may receive his per-

875, 905–06 (1991) (concluding that the common law remains a viable method of promoting legal changes that respond to societal needs).

184. For other articles proposing a new tort, see Natalie L. Regoli, *A Tort for Prying E-Eyes*, 2001 U. ILL. J.L. TECH. & POL'Y 267, 269 (suggesting that a new tort should be created that targets the "[s]urreptitious collection, storage, use and sale of personal data"); Jonathan P. Graham, Note, *Privacy, Computers, and the Commercial Dissemination of Personal Information*, 65 TEX. L. REV. 1395, 1419 (1987) (proposing a new tort of "commercial dissemination of private information" to protect information privacy).

185. *See, e.g.*, 5 U.S.C. § 552a(e) (2000 & Supp. 2006) (notice); *id.* § 552a(b) (choice); *id.* § 552a(d) (access); *id.* § 552a(e) (security). Professor Vincent Johnson argues that database owners have or should have a legal obligation to data subjects to safeguard personal data and to notify them when the security of their data has been breached. Vincent R. Johnson, *Cybersecurity, Identity Theft, and the Limits of Tort Liability*, 57 S.C. L. REV. 255, 263–64, 288 (2005). He bases the standard of care on federal and state data security statutes, tort principles, and the law of fiduciary duty. *Id.* at 264.

sonal information and control over the information revealed and how the recipient may use it. Accordingly, damages would be awarded based on injuries to the individual's choice and control.

The following sections examine these elements in turn.

A. *Potential Defendants: "One who Collects, Stores, Analyzes, or Trades"*

Potential defendants would include any entity that collects, stores, analyzes, or trades in personal information, and thus would specifically include data traders such as merchants, direct marketers, retail establishments, and travel agents. In other words, potential defendants would include every actor who maintains databases of personal information, except when the privacy policies of those actors are regulated by specific legislation that preempts common law. The data traders most susceptible to this tort would be merchants, service providers, and direct marketers, who currently are exempt from most legislation governing data privacy.

To the extent that a data trader functions as a consumer reporting agency (CRA), it will fall within the limitations of the Fair Credit Reporting Act (FCRA),[186] which would probably preempt any tort claims.[187] The FCRA defines CRAs as entities that assemble and sell credit or other information about individuals.[188] In the past, however, retail establishments have generally not been considered CRAs,[189] and it is not clear whether service providers (such as travel agents) or data brokers who collect and sell broad categories of data are considered CRAs. Thus, many of the data traders subject to tort liability for the misuse of information are not CRAs.

---

186. Fair Credit Reporting Act, 15 U.S.C. §§ 1681–1681x (2000 & Supp. 2006).

187. *Id.* § 1681t(a). Federal privacy laws are generally considered to be "floors" and have not preempted stronger state laws. In fact, many federal statutes explicitly allow states to enact stronger privacy protections. *See, e.g.*, Employee Polygraph Protection Act of 1988, 29 U.S.C. §§ 2001–2009 (2000); Telephone Consumer Protection Act of 1991, 47 U.S.C. § 227 (2000). *But see* Am. Bankers Ass'n v. Gould, 412 F.3d 1081, 1087 (9th Cir. 2005) (holding that the affiliate-sharing clause in FCRA partially preempts the stricter affiliate-sharing provision in California's Financial Information Privacy Act).

188. 15 U.S.C. § 1681a(f).

189. *See, e.g.*, Miller v. Trans Union Corp., 24 F. App'x 422, 424 (6th Cir. 2001) (concluding that neither a bank nor a tire company were CRAs under the FCRA because there was no evidence that either assembled or collected consumer data to distribute to third parties); Rush v. Macy's N.Y., Inc., 775 F.2d 1554, 1557 (11th Cir. 1985) (finding that department store was not a CRA because it only provided consumer information to a reporting agency and did not use it for profit).

CRAs generally may not use consumer credit reports for target marketing,[190] as FCRA restricts the distribution of consumer reports to applications for credit, insurance, and transactions initiated by the consumer.[191] However, FCRA allows CRAs to share the information in consumer reports with their corporate affiliates,[192] and permits CRAs to sell identifying information—name, mother's maiden name, date of birth, sex, address, previous address, Social Security number, and telephone number—when that information is not connected with a person's creditworthiness.[193] To the extent that a CRA is trading in data not specifically designated a consumer report by FCRA, the CRA might be subject to a tort claim, depending on a preemption analysis.[194] Further, the tort would apply to any affiliates who received personal information from a CRA, provided they are not themselves CRAs.

B. Information Protected: "Personal Information"

This tort would remedy the misuse of any personal information, broadly defined as any information that is linked with an individual. This definition includes full names, addresses, birthdates, Social Security numbers, biometrics, transactional data, travel data, work addresses, consumer preference or lifestyle profiles, telephone numbers—in short, any information collected, stored, analyzed, or produced by data traders, when it is or may be used to identify or contact an individual[195] (except where preempted by specific legislation, such as the regulation by FCRA of consumer reports).

Despite this broad definition of personal information, it is probably less likely that the tort will encounter First Amendment limitations similar to those that cabin the public disclosure and false light torts,

---

190. Trans Union Corp. v. FTC (*Trans Union I*), 81 F.3d 228, 234 (D.C. Cir. 1996).

191. 15 U.S.C. § 1681b(c). Credit reports may also be procured by court order, for employment purposes, and to state child support enforcement agencies. *Id.* § 1681b(a).

192. *Id.* § 1681a(d)(2)(A)(iii).

193. *Id.* § 1681b. A consumer report is defined as "bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living," which is used to establish the consumer's eligibility for credit, insurance, or employment. *Id.* § 1681a(d)(1). However, "[a] report limited solely to the consumer's name and address alone, with no connotations as to credit worthiness or other characteristics, does not constitute a 'consumer report.'" Commentary on the Fair Credit Reporting Act, 16 C.F.R. pt. 600, app. at 496 (2006).

194. The Ninth Circuit held that FCRA preempted state privacy law only insofar as it regulated the kind of information included in consumer reports—that is, information specifically regulated by FCRA. Am. Bankers Ass'n v. Gould, 412 F.3d 1081, 1086 (9th Cir. 2005).

195. *See supra* note 2.

precisely because this tort does *not* have a publicity requirement,[196] and it is almost beyond dispute that personal information of the sort traded by data brokers is not a matter of legitimate public interest (except in rare situations involving a public figure).[197]

The Supreme Court of the United States has not yet established how it will analyze limits and regulations placed on personal information that is used and traded in a commercial context. There are indications that such data is entitled to reduced First Amendment protection, either because it is speech that does not involve a matter of legitimate public interest, or because it is commercial speech.

In *Dun & Bradstreet, Inc. v. Greenmoss Builders, Inc.*,[198] a plurality of the court applied intermediate scrutiny to a defamation action concerning false data contained in a credit report.[199] In *Trans Union Corp. v. FTC* (*Trans Union II*),[200] the D.C. Circuit followed the reasoning of the *Dun & Bradstreet* plurality, applying intermediate scrutiny to

---

196. Eugene Volokh argues that government enforcement of Fair Information Practice codes would have troubling normative implications for the First Amendment: "Once people grow to accept and even like government restrictions on one kind of supposedly 'unfair' communication of facts, it may become much easier for people to accept 'codes of fair reporting,' 'codes of fair debate,' 'codes of fair filmmaking,' 'codes of fair political criticism,' and the like." Volokh, *supra* note 24, at 1116 (footnote omitted). His critique ignores the fundamental difference between speech such as reporting, debate, filmmaking, and political critique, which is conveyed to a general public, and speech conveyed between individuals that primarily serves an economic purpose. Further, his critique does not consider whether personal information, when sold as a commodity, is even speech. Neil Richards argues that many information privacy rules—such as one requiring data traders to secure their databases—have nothing to do with regulating speech but rather, can be viewed as regulating conduct, and further, that the regulation of "information flows" pursuant to a commercial relationship "is neither 'speech' within the current meaning of the First Amendment, nor should it be viewed as such." Neil M. Richards, *Reconciling Data Privacy and the First Amendment*, 52 UCLA L. REV. 1149, 1169 (2005) (footnotes omitted).

197. *Cf.* Dun & Bradstreet, Inc. v. Greenmoss Builders, Inc., 472 U.S. 749, 762 (1985) (plurality opinion) ("[T]here is simply no credible argument that [false] credit reporting requires special protection to ensure that 'debate on public issues [will] be uninhibited, robust, and wide-open.'"). Volokh argues that personal information is of great interest to people in "deciding how to behave in their daily lives, whether daily business or daily personal lives—whom to approach to do business, whom to trust with their money, and the like." Volokh, *supra* note 24, at 1115. The tort would not shut down this kind of information exchange; people interested in entering into business relationships with one another can voluntarily exchange information, or request that their data files be released to a third-party.

198. 472 U.S. 749 (1985) (plurality opinion).

199. *Id.* at 762. The plurality found that a wholly false credit report "was speech solely in the individual interest of the speaker and its specific business audience," which consisted of five corporate customers. *Id.* Accordingly, the credit reports were speech that "concern[ed] no public issue," and the award of presumed and punitive damages in the defamation action against Dun & Bradstreet, in the absence of actual malice, did not violate the First Amendment. *Id.* at 762–63.

200. 245 F.3d 809 (D.C. Cir. 2001).

regulation under FCRA of the sale of certain truthful "target marketing products" sold by Trans Union.[201] The products at issue were lists of names and addresses of individuals who met criteria—such as possession of a credit card with a $10,000 limit, car loan, or mortgage of a certain amount—specified by the purchaser of the list.[202] Trans Union compiled the lists from its credit databases, releasing the identifying information to the purchaser but withholding the credit details.[203] Purchasers of the data would know, however, that every person on the target list had met the creditor's criteria.[204] Examining the content, form, and context of the target lists, the court found that Trans Union's lists constituted speech unrelated to any public concern, which "is solely of interest to [Trans Union] and its business customers."[205] In *Trans Union Corp. v. FTC* (*Trans Union III*),[206] the court noted that the privacy concerns in Trans Union's case were significant because the lists contained names and addresses of individuals—not publicly traded corporations whose articles of incorporation and financial statements are generally open to public inspection.[207] Accordingly, the restriction under FCRA of the sale of the target marketing products directly served the substantial government interest of protecting the privacy of consumer credit information, and was no more extensive than needed to serve that interest.[208]

The implications of the *Trans Union* decisions are that regulations on the sale of truthful data that exceeds basic identifying information (i.e., transactional or travel data, or personality profiles) will be subjected to intermediate First Amendment scrutiny, provided that the data's content, form, and context reveal no matters of public concern, and that the protection of individual consumer privacy will likely qualify as a substantial government interest. The *Dun & Bradstreet* plurality opinion also suggests that presumed and punitive damages are not a more extensive regulation than needed by the state to protect that interest.[209]

---

201. *Id.* at 818.

202. *Id.* at 815.

203. *Id.* at 812.

204. *Id.* Because these lists qualified as consumer credit reports, the FTC prohibited Trans Union from selling them. *Id.* at 812–13.

205. *Id.* at 818.

206. 267 F.3d 1138 (D.C. Cir. 2001).

207. *Id.* at 1140.

208. *See id.* at 1142–44; *Trans Union II*, 245 F.3d at 819. *But see* Equifax Servs., Inc. v. Cohen, 420 A.2d 189, 200 (Me. 1980) (invalidating parts of the Maine Fair Credit Reporting Act for failing to advance a substantial government interest and for regulating speech more extensively than is necessary).

209. *Dun & Bradstreet*, 472 U.S. at 763.

The *Dun & Bradstreet* plurality specifically declined to find that credit reports were commercial speech, although it discussed commercial speech cases to show that the arguments in favor of reduced protection for commercial speech similarly apply to credit reports.[210] Thus it is still possible that lists of personal information sold or rented for marketing purposes could be treated as commercial speech and subject to the test outlined by the Supreme Court in *Central Hudson Gas & Electric Corp. v. Public Service Commission*.[211] According to the *Central Hudson* Court, to receive First Amendment protection, the speech must concern lawful activity and not be misleading; in addition, the government must have a substantial interest in regulating the speech, and the regulation cannot be more extensive than necessary to serve that interest.[212] It is difficult to predict how an indirect regulation (like a tort) on the commercial use of personal information would fare under the first part of this test, because the speech in question (the information) does not concern an activity so much as an identity, and it does not propose a commercial transaction so much as convey a commodity (the identity itself) that will eventually be used in the process of proposing a commercial transaction.[213] If it were considered protected commercial speech, however, it is likely that the tort would survive *Central Hudson* intermediate scrutiny given the substantial government interest in protection of information privacy and that a tort claim for damages is not a more extensive regulation than necessary to protect the interests of the individual who has been harmed.

Finally, it is also possible that the personal information used by data traders is not even "speech" protected by the First Amendment.[214] The *Central Hudson* Court emphasized that the concern for commercial speech in the First Amendment is based on the power of

---

210. *Id.* at 762 & n.8. Commercial speech cases have, for the most part, concerned advertisements, although commercial speech is defined more broadly as "expression related solely to the economic interests of the speaker and its audience." Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n, 447 U.S. 557, 561 (1980). The Tenth Circuit has twice found that restrictions on the commercial use of personal data implicated the First Amendment. *See* Mainstream Mktg. Servs. v. FTC, 358 F.3d 1228, 1233 (10th Cir. 2004) (holding that the national "do-not-call registry [wa]s a valid commercial speech regulation," noting, in part, that the list restricted "only core commercial speech—i.e., commercial sales calls"); U.S. West, Inc. v. FCC, 182 F.3d 1224, 1239 (10th Cir. 1999) (holding that regulations requiring telephone services providers to get the affirmative consent of their customers before using CPNI for direct marketing were invalid commercial speech regulations).

211. 447 U.S. at 566.

212. *Id.*

213. *But see U.S. West*, 182 F.3d at 1232–33 (reasoning that telephone carriers wanted to use CPNI for commercial solicitation, so any restriction on the use of CPNI is a restriction on commercial speech).

214. Richards, *supra* note 196, at 1152.

speech to inform the public, even as it simultaneously serves the speaker's economic interests.[215] This focus on informing the public suggests that commercial speech that is not publicly disseminated, but rather distributed solely as an incident of a commercial transaction, might not receive any First Amendment protection.[216] A possible example of such treatment occurred in *Reno v. Condon*,[217] in which the Supreme Court found that the personal information covered by the Driver's Privacy Protection Act—photograph, Social Security number, driver identification number, name, address, and telephone number—was, in the context of its sale and resale, "an article of commerce."[218] Because the information was a commodity, Congress could subject its use in commerce to reasonable regulations. The issue in *Reno* was federalism—whether Congress had the power to regulate information as commerce—and the parties did not raise First Amendment questions. If the Court were to conclude that personal information as used by data traders is a commodity, not speech, a tort that indirectly regulates the use of that commodity would be tested under the principles of substantive economic due process and equal

---

215. *Cent. Hudson*, 447 U.S. at 561–62. The Court noted that:

> Commercial expression not only serves the economic interest of the speaker, but also assists consumers and furthers the societal interest in the fullest possible dissemination of information. In applying the First Amendment to this area, we have rejected the "highly paternalistic" view that government has complete power to suppress or regulate commercial speech. "[P]eople will perceive their own best interests if only they are well enough informed, and . . . the best means to that end is to open the channels of communication, rather than to close them. . . ." Even when advertising communicates only an incomplete version of the relevant facts, the First Amendment presumes that some accurate information is better than no information at all.

Id. (citations omitted).

216. *Cf.* Ohralik v. Ohio State Bar Ass'n, 436 U.S. 447 (1978). The Court opined that:

> [I]t has never been deemed an abridgment of freedom of speech or press to make a course of conduct illegal merely because the conduct was in part initiated, evidenced, or carried out by means of language, either spoken, written, or printed. Numerous examples could be cited of communications that are regulated without offending the First Amendment, such as the exchange of information about securities, corporate proxy statements, [and] the exchange of price and production information among competitors . . . .

Id. at 456 (citations and internal quotation marks omitted); *see also* L.A. Police Dep't v. United Reporting Publ'g Corp., 528 U.S. 32, 40 (1999) (upholding state law that restricted media access to identifying information about arrestees).

217. 528 U.S. 141 (1999).

218. *Id.* at 148.

protection law. It is almost certain that the tort would survive rational basis review.[219]

C. *Standard of Care: "The Failure to Use Fair Information Practices"*[220]

The tort would impose a minimum standard of care on private entities to abide by the same standards of Fair Information Principles—notice, choice, access, and security[221]—that bind the federal government. The principles of Fair Information Practice were developed in the 1970s by a government task force grappling with the management of enormous government databases.[222] These four principles were implemented in the Privacy Act of 1974,[223] which governs the collection, storage, processing, and disclosure of personal information by federal agencies. These practices, while somewhat bare bones,[224] have the advantage of being globally accepted and long established[225] and, thus, would provide few surprises to data traders (indeed, the DMA has already pledged its commitment to using such practices).[226]

---

219. *See* Richards, *supra* note 196, at 1171–73 (positing that fair information regulations should be subject to the low level scrutiny employed by courts in other contexts—i.e., rational basis review).

220. Although this tort has been presented using the language of negligence, the argument could be made for creating a strict liability tort, particularly because of the cost and difficulty of administering a negligence regime. *See* Epstein, *supra* note 180, at 28–30.

221. *See* Gellman, *supra* note 25, at 195–202 (discussing the statutory codes under the Privacy Act of 1974 that set forth the rules governing "the collection, maintenance, use, and disclosure of personal information held by federal agencies").

222. *See generally* ADVISORY COMM. ON AUTOMATED PERS. DATA SYS., U.S. DEP'T OF HEALTH, EDUC. AND WELFARE, RECORDS, COMPUTERS AND THE RIGHTS OF CITIZENS (1973), *available at* http://www.epic.org/privacy/hew1973report.

223. 5 U.S.C. § 552a (2000 & Supp. 2006); *see also* PRIVACY PROTECTION STUDY COMMISSION, *supra* note 77, at 500–03 (outlining the elements of the Privacy Act and evaluating the implementation of revisions).

224. Since the 1970s, various government agencies have issued refined lists of Fair Information Practices. In the online context, the FTC described them as (1) Notice/Awareness; (2) Choice/Consent; (3) Access/Participation; (4) Integrity/Security; and (5) Enforcement/Redress. FTC, PRIVACY ONLINE: A REPORT TO CONGRESS 7–11 (1998), *available at* http://ftc.gov/reports/privacy3/priv-23a.pdf. More recently, the Department of Commerce described its own set of principles in the context of companies that want to qualify as "safe harbors" that can receive data from companies bound by the European Data Directive. U.S. DEP'T OF COMMERCE, SAFE HARBOR PRIVACY PRINCIPLES (2000) [hereinafter SAFE HARBOR PRIVACY PRINCIPLES], *available at* http://www.export.gov/safeharbor/SH-PRINCIPLESFINAL.htm. The principles include notice, choice, access, security, data integrity, enforcement, and "onward transfer," which requires the safe harbor company to determine that any third party to which it transfers data follows these principles. *Id.*

225. *Cf.* Gellman, *supra* note 25, at 213–15 (noting the influence of U.S. privacy policies on international privacy standards).

226. *See supra* notes 81–86 and accompanying text.

In addition, using the principles of Fair Information Practices as a standard of care emphasizes that the tort targets a data trader's *misuse* of data, rather than the mere collection or possession of data (unless the data were obtained surreptitiously, as by pretexting).[227] Instead, the tort targets data abuses occurring at the analysis and use stages of the data flow, including the unauthorized sale, renting, or mining of personal information, and its negligent release.[228] The charts in the Appendix that follow this Article correlate the principles of Fair Information Practices with liability for misuse.

1. *The Choice Principle*

The choice principle would compel data traders to seek the consent of their data subjects before using personal information obtained for one purpose in a way that is incompatible[229] with that purpose.[230] The choice principle provides that there must be a way for an individ-

---

227. *See* Zarsky, *supra* note 28, at 32–33 (asserting that reform efforts should not be concentrated on the collections stage of data trading). Professor Zarsky argues that "[s]ince any form of regulation within this context will be met with strong and powerful opposition, legislation must be pragmatic and focus its concern on the actual detriments that may occur. Solutions should protect the public from dangerous uses of personal information, rather than mere surveillance." *Id.*

228. *See id.* at 17–32 (dividing the data flow into three discrete stages: collection, analysis, and use or implementation).

229. The compatibility standard is part of the Privacy Act, which requires a government agency to tell individuals the principle purpose or use of the information it collects, to explain the "routine use" that may be made of the information, and to publish a notice in the Federal Register that specifically describes the routine uses of records it maintains. 5 U.S.C. § 552a(e)(3)–(4). A routine use must be "compatible with the purpose for which [the information] [i]s collected." *Id.* § 552a(a)(7). This means that there must be a "concrete relationship or similarity, some meaningful degree of convergence, between the disclosing agency's purpose in gathering the information and in its disclosure." Britt v. Naval Investigative Serv., 886 F.2d 544, 549–50 (3d Cir. 1989); *see also* Covert v. Harrington, 876 F.2d 751, 755–56 (9th Cir. 1989) (determining that the Department of Energy's disclosure of nuclear employees' personnel security questionnaires to Department of Justice, for the purpose of criminal prosecution, violated the Privacy Act because the Department did not notify the employees that the questionnaire could be used for law enforcement purposes; rather, employees were expressly told that the information would be used only for security clearance purposes); Mazaleski v. Treusdell, 562 F.2d 701, 713 n.31 (D.C. Cir. 1977) (suggesting that the communication to a prospective employer of derogatory information concerning a former federal employee's dismissal is not compatible with the purpose for which the information was collected); S. REP. NO. 93-1183, at 69 (1974) (recognizing that the Privacy Act "prevents an agency from merely citing a notice of intended 'use' as a routine and easy means of justifying transfer or release of information"). The routine use standard has been described as a "gaping loophole" in the Privacy Act. Kang, *supra* note 22, at 1271; *see also* Nehf, *supra* note 25, at 41–42 (calling the routine use standard a "glaring failure").

230. Based on a detailed economic analysis, Professor Kang concludes that, as a "default rule," the "information collector should process data only in functionally necessary ways," unless the parties agree otherwise. Kang, *supra* note 22, at 1259.

ual to prevent information about him obtained for one purpose from being used or made available for other purposes without his consent.[231]

The choice principle would allow individuals to limit meaningfully the secondary uses of their data, including sale, rental, aggregation, profiling, and mining, because without the explicit consent of the data subject, the data trader would become liable for these practices. Thus, a retailer who collects information for one use (the purchase and shipping of a classical music CD) and sells or rents it for another (direct marketing of similar CDs) would violate the standard of care.[232] Construed broadly, this principle would prevent data sharing between affiliates (unless preempted by a statute such as FCRA or GLBA), and might even require the retailer to obtain consent before using purchasing information for future direct marketing of his own products.

The practical effect of the choice principle is to force data traders to discover—and honor—the privacy preferences of their data subjects. A self-imposed, low-cost, and effective way to do so would be to establish a clearinghouse Website or hotline (similar to the national Do-Not-Call list or OptOutPrescreen.com) that would allow individuals to indicate their data privacy preferences. Presumably, these preferences could range from strong privacy preferring (an almost total restriction on data use except for functionally necessary[233] purposes) to weaker privacy preferring (permitting aggregation, profiling, or permitting data sharing with third parties). Data traders would be motivated to participate in such a system because it facilitates discovering the privacy preferences of their data subjects, has national application, and would not entail comprehensive government regulation.

---

231. *See* SAFE HARBOR PRIVACY PRINCIPLES, *supra* note 224 (setting forth the choice principle).

232. Currently, this type of incompatible use is subject to FTC regulation, but only if the data trader violates its own privacy policy. Zarsky, *supra* note 28, at 26.

233. Kang defines functionally necessary uses, particularly as related to commercial transactions in cyberspace, in the following way:

> [S]uccessful communication between parties; successful payment and delivery between parties, including accounting and debt collection through independent contractors; successful dispute resolution between parties . . . ; warnings to the individual of any defect or danger; maintenance of the information collector's cyberspace infrastructure; protection of the collector from fraud and abuse; and adherence to governmental recordkeeping regulations . . . .

Kang, *supra* note 22, at 1271–72. Functional necessity does not include future direct advertising from the information collector to the data subject, unless the subject specifically agrees to this use. *Id.* at 1272.

2. *The Notice and Access Principles*

The notice and access principles would require data traders to notify individuals of the types of information they collect, the uses being made of their information, and to give individuals access to their data profiles.[234] The notice principle provides that there must be no personal data record-keeping systems whose very existence is secret,[235] which suggests that data subjects must be able to discover the types of records that a company keeps, and particularly those that include an individual's information. The access principle provides that there must be a way for an individual to find out what information about him is in a record and how it is used, and a way for an individual to correct or amend a record of identifiable information about him.[236]

Notice and access to secondary uses of data are especially important if individuals are to effectively police the accuracy of their data profiles and investigate whether data traders are honoring their privacy choices. Currently, it is difficult, if not impossible, for individuals to gain access to their data files—even when they have been notified that the security of the file has been compromised.[237] Thus, for example, individuals should not only have access to their personal information, but they should also have access to a list that reveals whether their data has been mined, sold, or rented, and if so, to whom. They should also have access to their personality profiles, and to the results of any mining, provided such access does not reveal anyone else's personal information.[238] Data traders would not be liable for creating profiles, provided that they do so with the individual's consent, or for

---

234. I disagree that profiles are fully the "property" of the data traders who created them, in the sense that they have the right to exclude all others from seeing the profiles, especially the subjects of the profiles. Zarsky, *supra* note 27, at 29 n.91. Although the data trader has compiled the profile and probably owns a copyright in that profile, the individual who is the subject of the profile bears the risk of any of its inaccuracies and insults, and Fair Information Practices require that she be notified of and able to access that profile. A sensible compromise between the competing interests of the individual and the data trader would be to allow individuals to access only their own profiles, to prohibit copying of the profiles except for personal use, and to permit data traders to conceal their methods or processes of analysis (i.e., their algorithms, or anything protected as trade secrets).

235. *See* SAFE HARBOR PRIVACY PRINCIPLES, *supra* note 224 (setting forth the notice principle).

236. *See id.* (setting forth the access principle).

237. *See supra* note 88 and accompanying text.

238. I am less convinced than Zarsky about the benefits of preserving a company's free analysis of information, especially when companies like Axciom advertise that they analyze data into ethnic and racial categories. Zarsky, *supra* note 28, at 38; *see also* Reidenberg, *supra* note 1, at 883 (describing Axciom's product catalog). Plaintiffs who suspect that their personal information has been used to support some form of invidious discrimination particularly need to know how data traders have analyzed their information.

the content of the profiles, provided they are otherwise legal; rather, they would be liable for refusing to provide notice of and access to the profiles.

3. The Security Principle

Finally, the security principle would hold data traders liable for the negligent handling and protection of personal data. The security principle provides that any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for its intended use and must take reasonable precautions to prevent misuse of the data.[239] Under this standard, a plaintiff could recover if injured by a data trader's negligent security breach, as in the LexisNexis or Bank of America situations—or by the negligent sale of information to third parties who have no legitimate interest in seeing it, including criminals, as in the ChoicePoint situation—or exposure of data to foreseeable security risks during processing, such as permitting certain inmates to process data in prison.[240]

Presumably, courts wrestling with information privacy torts would refine these four principles, seeking guidance from privacy standards in other federal or international laws. The European Data Directive, for example, additionally requires that data be stored for no longer than necessary and prohibits the processing (analysis or mining) of certain suspect categories of data, such as racial or ethnic origin, political opinion, religious or philosophical belief, or health and sex life.[241] Incorporation of this principle would effectively limit the mining or analysis of these suspect categories of information.

Finally, this standard of care could not be waived by agreement, and thus would obligate data traders to deal fairly with the personal information they already have in their databases, regardless of how obtained or created—from public records or information provided by the individual with or without the consent of the individual. Because the standard of care is a mandatory rule, it resolves the problem of how to force data traders to deal fairly with the vast quantities of data obtained from public records before more stringent privacy regulations (such as the DPPA) were enacted, or from consumers who may

---

239. *See* SAFE HARBOR PRIVACY PRINCIPLES, *supra* note 224 (setting forth the security principle).

240. *See, e.g.*, Stanley S. Arkin, *Misuse and Misappropriation of Electronically Stored Information*, N.Y. L.J., July 23, 2001, at 3 (discussing the Metromail settlement in which Metromail was sued by a woman who was stalked by a former inmate who had processed her personal data while in prison).

241. Council Directive 95/46, art. 8, 1995 O.J. (L 281) 31, 40–41 (EC).

be unaware that companies are collecting information about them or about how that information will be used. Many commentators have focused on protecting data at the collection stage of the data flow, advocating opt-in systems that force data traders to obtain consumer consent to their information practices.[242] Ideally, this system allows consumers to choose from a menu of privacy options, which could then be policed. But a weakness of the consent-based approach is that it does not require data traders to treat fairly the data they have already collected without the subject's consent, or with consent to extremely unfair information practices. Clearly, it would be unfair to hold data traders liable *now* for previously creating a data profile; however, once an individual discovers that such a profile exists and expresses her objection to it, the data trader would have to delete the profile and cease any further aggregation or mining of that individual's information.

One further objection to this standard of care is that it imposes a mandatory assumption about privacy preferences, when individual choice is integral to the very notion of privacy it imposes.[243] However, the critical mandate of the Fair Information Practices standard is that individuals *must have* a meaningful choice about how their data is used. Only the *choice itself* is not waivable; individuals would still be free to select greater or lesser privacy preferring options for the uses of their data, or indicate a strong privacy preference for certain entities such as data brokers but allow for more information processing by trusted businesses so that they can enjoy certain conveniences. Thus, for example, while an individual might choose not to permit ChoicePoint to aggregate or mine her personal information, she might permit Amazon.com to do so because she enjoys receiving reading suggestions.

---

242. *E.g.*, McClurg, *supra* note 8, at 128–37; Cohen, *supra* note 20, at 1432–35 (defining consent for the purposes of accessing personally identifiable data).

243. *See* Kang, *supra* note 22, at 1266. Professor Kang notes that "control is at the heart of information privacy," and that "the state should hesitate to proscribe information flow on some paternalistic theory." *Id.* He concedes, however, that paternalistic intervention would be justified if the empirical data exists to show that Americans "systematically overvalue[ ]the short-term benefit of disclosing personal information . . . and undervalue[ ] the long-term harm of detailed profiles." *Id.* at 1266 n.301.

Professor Schwartz, operating on a property theory, would impose a limit on the free alienability of data. Schwartz, *supra* note 20, at 2097. His property scheme limits the alienability and future uses of personal information, so that the individual's property interest "runs with the asset." *Id.*

D. Damages

The new tort protects the individual's inherent right to control her personal information, and thus would award damages based on emotional loss, monetary loss, or both.

In past litigation, damages in privacy cases have been difficult to prove or have been considered so minimal that the cases do not justify the litigation expenses.[244] The *Restatement* approach to damages for privacy torts is based on the law of defamation: it allows for general damages, which are not linked to any specific monetary harm, for the harm to the privacy interest that was invaded and mental distress resulting from the invasion,[245] and special damages (actual, material, or monetary losses) caused by the invasion.[246] On paper, this approach seems to be sufficiently flexible to redress the many varieties of injury that may be caused by the misuse of personal information: financial (the consequences of identity theft or price discrimination), emotional (injury to dignity, seclusion, or reserve; mental distress), and a combination of both (anxiety about identity theft that results in medical expenses).

Thus, returning to the four scenarios at the beginning of this Article, the woman frightened by the inmate, the man offended by unsolicited advertisements, and the woman offended by learning about her consumer profile would receive general damages compensating the harm to their interest in controlling how their personal information is used and any mental distress that resulted from the loss of control. The law student could recover for his financial losses, the time spent clearing up the identity theft, and mental distress.

For the damages to be effective—i.e., provide sufficient incentives to force the data traders to reform their privacy practices—plaintiffs must be able to bring class actions based on aggregates of harm.[247]

---

244. *See, e.g.*, Schwartz, *supra* note 20, at 2108 (discussing the difficulty of proving actual damages in the privacy context, and noting that "an individual's personal data may not have a high enough market value to justify the costs of litigation").

245. RESTATEMENT (SECOND) OF TORTS § 621, § 652H cmt. b (1977). Certain defamation torts require proof of "special harm" of a material or pecuniary nature before general damages can be awarded. *Id.* § 575 cmts. a & b.

246. *Id.* § 652H cmt. d.

247. Damages for harms to privacy interests are so difficult to quantify that even classes of plaintiffs have failed to plead sufficient injury. For example, in the *DoubleClick* litigation, the claim under the Computer Fraud and Abuse Act was dismissed because the plaintiffs failed to allege losses of $5,000, the statutory minimum, to one or more individuals during any one-year period. *In re* DoubleClick, Inc. Privacy Litig., 154 F. Supp. 2d 497, 523 (S.D.N.Y. 2001). The court interpreted 18 U.S.C. § 1030(e)(8)(A) (2000) to permit plaintiffs to aggregate damages "across victims and over time for a single act" that violated the statute, but not across all victims and all acts for any given year. *Id.* More recently, how-

The purpose of consumer class action lawsuits is to "aggregate[ ] numerous small claims into one action," thereby enhancing judicial efficiency and access to the courts.[248] Class action lawsuits arising from violations of information privacy serve both the efficiency and access goals. But because the likely damages for even a successful suit for misuse of personal information are small, individual plaintiffs are, practically speaking, precluded from seeking a remedy without the possibility of aggregating harm.[249]

Ideally, state or federal legislation[250] would eventually impose a scheme of damages similar to that in the copyright statute.[251] Under this type of scheme, the proof of misuse of personal information would give rise to general or presumed damages, in a statutorily imposed range, if the defendant acted negligently.[252] A higher range of damages would be available if the data trader behaved willfully.[253] The FCRA also provides a useful model for privacy remedies. Under the FCRA, individuals have a right of access to their credit reports, the right to correct inaccurate information, the ability to opt out of prescreened credit "opportunities,"[254] and a private right of action against CRAs with remedies including minimum damages, attorneys' fees, and punitive damages.[255]

---

ever, the Eleventh Circuit held that the DPPA, which has a liquidated damages provision, did not require proof of actual damages, and allowed a class action against a savings bank that had illegally purchased motor vehicle records from the state to proceed. Kehoe v. Fid. Fed. Bank & Trust, 421 F.3d 1209, 1216–17 (11th Cir. 2005), *cert. denied*, 126 S. Ct. 1612 (2006).

248. Weld v. Glaxo Wellcome Inc., 746 N.E.2d 522, 532 (Mass. 2001).

249. *Id.*

250. Professor Froomkin argues that statutorily imposed damages schemes would create a sufficient incentive for individuals to police the privacy policies of data traders. Froomkin, *supra* note 25, at 1528. Many privacy statutes include provisions for liquidated or minimum damages. *See, e.g.*, 18 U.S.C. § 2710(c)(2) (2000); 18 U.S.C. § 2724(b)(2) (2000 & Supp. 2006); 47 U.S.C. § 551(f)(2) (2000 & Supp. 2006). The Privacy Act has a similar provision, 5 U.S.C. § 552a(g)(4) (2000 & Supp. 2006), but "plaintiffs must prove some actual damages to qualify for a minimum statutory award of $1,000." Doe v. Chao, 540 U.S. 614, 616 (2004).

251. *See, e.g.*, 17 U.S.C. § 504 (2000 & Supp. 2006) (stating that a copyright infringer "is liable for either (1) the copyright owner's actual damages and any additional profits . . . or (2) statutory damages, as provided by subsection (c)").

252. *See id.* § 504(c)(1) (providing a damages range of $750 to $30,000).

253. *Id.* § 504(c)(2) (permitting courts to increase statutory damages up to $150,000 for willful copyright infringements).

254. 15 U.S.C. § 1681b(e) (2000 & Supp. 2006). One may opt out by going to https://www.optoutprescreen.com (last visited Oct. 10, 2006).

255. 15 U.S.C. § 1681n.

VI. CONCLUSION

The development of sexual harassment law provides a useful historical model for using a judge-made remedy to redress a social wrong that the legislature has not—or will not—address. Because the common law did not recognize sexual harassment as a cause of action, prior to the enactment of Title VII of the Civil Rights Act of 1964 (Title VII),[256] individuals used traditional common law actions such as wrongful discharge, breach of contract, intentional infliction of emotional distress, or intentional interference with contractual relations to bring indirectly the types of claims that now can be brought directly under Title VII.[257] The common law thus preceded the public law, acting as a "crowbar" for reform and accountability. The traditional common law claims ultimately were an imperfect fit with the particulars of sexual harassment claims, but the precedent provided a useful laboratory for the sweeping federal legislation to come and for its subsequent interpretation. Coming full circle, commentators are urging now that the common law should recognize a tort of sexual harassment.[258]

Admittedly, the judicial administration of a problem as pervasive as information misuse could be a nightmare for the courts and data traders. But, for people whose information has been misused, the current system—or non-system—is already a nightmare.[259] There have been enormous losses, both direct (the estimated cost of identity theft in time and money and the psychological harm caused by loss of control over one's identity) and indirect (the opportunity costs of people avoiding electronic commerce because they fear identity theft or loss of control over their personal information). The data traders are currently free riding on the information of others because—except in rare circumstances such as the ChoicePoint example—they do not shoulder the full costs of their inaccuracies and security leaks. Instead, individuals shoulder the burden, paying with their time, money,

---

256. Civil Rights Act of 1964, 42 U.S.C. §§ 2000e-1 to -17 (2000).

257. *See* Sarah E. Wald, *Alternatives to Title VII: State Statutory and Common-Law Remedies for Employment Discrimination*, 5 HARV. WOMEN'S L.J. 35, 44–59 (1982) (discussing common law contract and tort claims available when Title VII and state antidiscrimination statutes are unavailable); Christopher P. Barton, Note, *Between the Boss and a Hard Place: A Consideration of* Meritor Savings Bank, FSB v. Vinson *and the Law of Sexual Harassment*, 67 B.U. L. REV. 445, 463 (1987) (noting that prior to the enactment of Title VII, as well as now, plaintiffs may bring claims of sexual harassment under the traditional tort rubric).

258. *E.g.*, Ellen Frankel Paul, *Sexual Harassment as Sex Discrimination: A Defective Paradigm*, 8 YALE L. & POL'Y REV. 333, 362 (1990) (proposing a tort of sexual harassment that is based on the tort of intentional infliction of emotional distress).

259. *See "Who Am I?"*, *supra* note 19 (detailing the difficulties of trying to clear one's credit report after identity theft).

and injuries to their choice and control. It is not only fair, but also logical, that the person who suffers the harm from information misuse should have control of how her personal information is used. It also makes sound economic sense to create a viable protection for consumer data privacy, as injured or fearful consumers will hesitate to consume in ways that make them more vulnerable to information abuse, forgoing Internet and other forms of electronic commerce.

Realistically, the data traders would not be helpless when faced by classes of angry plaintiffs. As in other areas of tort, data traders would have the opportunity to develop mitigating defenses. For example, a data trader may have a viable defense when it followed Fair Information Practices but was defrauded and consequently sold information to someone not entitled to receive it, or when its highly secure database is improbably hacked or compromised by a virus. Furthermore, courts would probably develop a "cure" defense: the data trader's prompt "cure" of a problem, such as data inaccuracy, might release it from liability for damages. Additionally, individuals would be expected to take responsibility for making their privacy preferences known and for keeping their personal information secure (a contributory negligence or comparative fault defense). Finally, insurance companies already provide insurance against "data intrusion";[260] insurance against data misuse would surely develop.

The most positive effect of a new tort would be the creation of an incentive for data traders to invest in better data security technologies and to take seriously their obligation to use Fair Information Practices.[261] A viable personal information tort would force data traders to implement better systems of obtaining consumer consent to the collection and use of their personal information. After a few successful lawsuits for the misuse of personal information, data traders would realize that they must obtain consent for data processing, requiring them to discover the privacy preferences of their data subjects and motivating them to seek a self-imposed solution.

Ironically, a patchwork of common law tort regimes may have data traders begging for comprehensive federal legislation. Ultimately, sweeping federal legislation will be the most effective way to rein in the data traders, given the portability of data, the pervasiveness of the current problems, and the inevitability that misuses will increase as data technology grows ever more sophisticated. However,

---

260. *See, e.g.*, Johnson, *supra* note 185, at 277–78 & n.143 (noting that insurance companies are offering data intrusion policies).

261. *See* Froomkin, *supra* note 25, at 1528, 1540 (urging the creation of mechanisms to create incentives for the self-policing of privacy policies).

even an imperfect common law claim may provide a small foothold on a remedy for individuals who have been harmed but currently have no recourse to redress that harm. And, as the history of employment discrimination litigation shows, that legislation will be better constructed if it is built on the experience of the common law.

APPENDIX 1

Fair Information Practices correlated with liability for misuse of personal information

	Fair Information Practices	Tort of Misuse
NOTICE	There must be no personal data record-keeping systems whose very existence is secret.	Data traders maintain secret databases of information.
CHOICE	There must be a way for an individual to prevent information about him obtained for one purpose from being used or made available for other purposes without his consent.	Data is combined, profiled, analyzed, mined, rented, or sold without the consent of the data subject or in ways incompatible with original purpose. Data trader continues to sell or process data after individual has objected or otherwise indicated her privacy preferences
ACCESS	There must be a way for an individual to find out what information about him is in a record and how it is used. There must be a way for an individual to correct or amend a record of identifiable information about himself.	Data trader refuses to grant access to files, fails to make prompt corrections, or maintains inaccurate information.
SECURITY	Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for its intended use and must take reasonable precautions to prevent misuse of the data.	Data trader fails to implement and maintain appropriate technological measures to protect data against accidental loss, unauthorized alteration, disclosure, access, or dissemination to persons with no legitimate need for the data.

Appendix 2

An expanded view of Fair Information Practices correlated with liability for misuse

	Fair Information Practices & other U.S. Laws	European Union Data Privacy Directive 95/46, 1995 O.J. (L281) 32 (EC)	Tort of Misuse
NOTICE	There must be no personal data record-keeping systems whose very existence is secret.		Data traders maintain secret databases of information.
CHOICE	There must be a means for an individual to prevent information obtained about him for one purpose from being used or made available for other purposes without his consent. FCRA, 15 U.S.C. § 1681b(e) (2000 & Supp. 2006): consumer must be able to "opt out" of prescreened credit opportunities	Article 6(b): Data should not be processed in a way incompatible with the purposes for which it was collected. Article 7(a) and 14(b): Data subject must unambiguously consent to the processing of his data, and be able to object to data processing for the use of direct marketing.	Data is combined, profiled, analyzed, mined, rented, or sold without the consent of the data subject or in ways incompatible with original purpose. Data trader continues to sell or process data after consumer has objected or opted out.
ACCESS	There must be a means for an individual to find out what information about him is in a record and how it is used. There must be a way for an individual to correct or amend a record of identifiable information about himself.	Article 12: Data subject must be able to access, demand corrections, and block the further processing of data. Article 6(d): Data should be complete, accurate and, where necessary, up to date.	Data trader refuses to grant access to files, fails to make prompt corrections, maintains inaccurate or outdated information.
SECURITY	Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for its intended use and must take reasonable precautions to prevent misuse of the data.	Article 17: Data controller must implement appropriate technological measures to protect data against accidental loss and unauthorized alteration, disclosure, or access, especially if processing involves transmission over a network.	Data trader fails to implement and maintain appropriate technological measures to protect data against accidental loss, unauthorized alteration, disclosure, access, or dissemination to persons with no legitimate need for the data.

OBSOLETE DATA	FCRA, 15 U.S.C. § 1681c(a): CBAs must purge adverse credit information more than seven years old.	Article 6(e): Data should be kept in a personally identifying way for no longer than is necessary for the original purposes or for further processing.	Data trader fails to purge information in appropriate and timely manner.
CATEGORIES OF DATA THAT RAISE CONCERNS ABOUT DISCRIMINATION	Equal Credit Opportunity Act, 15 U.S.C. § 1691 (2000): prohibits credit discrimination on basis of race, color, religion, national origin, sex, marital status, welfare payments, or age.	Article 8: Certain data will not be processed: racial or ethnic origin, political opinion, religious or philosophical beliefs, trade union membership, health, or sex life.	Data trader processes, sells, or otherwise trades or exchanges information about race, color, religion, national origin, sex, marital status, welfare payments, or age.
PROTECTION OF CHILDREN	Children's Online Privacy Protection Act, 15 U.S.C. § 6501 (2000): limits collection and further use of information collected about children.		Data trader collects any information from or about children.