Case Western Reserve Journal of Law, Technology & the Internet
Volume 1, Number 1 Fall 2009

COMPREHENSIVE DATA PRIVACY LEGISLATION: WHY NOW IS THE TIME?

Tanith L. Balaban[*]

TABLE OF CONTENTS

I. INTRODUCTION

We live in a society that never forgets. By the time one dies, there will be a complete list of every web search he or she has done, everything he or she has bought, every place he or she has lived, every car he or she has owned, and so forth. This information will be connected to each person he or she has ever known and all of their web searches, purchase history, and so

[*] Associate Attorney, Gordon & Rees L.L.P.; J.D., *cum laude*, Case Western Reserve University School of Law, 2008; B.A., University of Arizona, 1999.

forth, by software and databases scattered across the globe. This is so because "[b]oth on and offline, businesses are collecting … staggering amounts of personal information about American citizens and compiling it into electronic dossiers designed to predict the way people think and behave."[1] The compilation and aggregation of personal information is standard operating procedure for companies and is done largely without consumer consent.[2] One commentator noted that "[t]he extent to which an individual's personal information is on display is startling: an average American's information can be found in anywhere between twenty-five and one hundred commercial databases."[3] United States companies, which are subject only to rudimentary data regulation, amass this information because an individual's personally identifiable information has tremendous value. Even for manufacturing businesses, the processing of information about goods sold and the identities of customers is now just as important as the production and shipping of the goods themselves. Data collection companies such as ChoicePoint make their money solely by selling "information about consumers to employers, marketers and others."[4] The public at large contributes to this system each time an individual conducts a Google search, makes a purchase online, creates a Facebook profile or even records a television show. The general public's

---

[1] Andrew J. McClurg, *A Thousand Words Are Worth a Picture: A Privacy Tort Response to Consumer Data Profiling*, 98 NW. U. L. REV. 63, 65 (2003); *see also* Milt Freudenheim, *And You Thought a Prescription Was Private*, N.Y. TIMES, Aug. 8, 2009, *available at* http://www.nytimes.com/2009/08/09/business/09privacy.html (explaining how prescriptions and the underlying information including the patients' names and addresses, dosages, social security numbers, and the names of the doctors, are bought and sold, often without the patients' knowledge or permission).

[2] This information is also sold in the underground economy. For example, a recent report shows that a full identity sells for between seventy cents and sixty dollars, bank account information sells for between ten dollars and one thousand dollars, email accounts sell for between ten cents and one hundred dollars, and credit card information sells for between six cents and twenty dollars. *See* Dean Turner et al., *Symantec Internet Security Threat Report: Trends for 2008*, *in* 14 SYMANTEC SECURITY 82 (2009), *available at* http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiv_04-2009.en-us.pdf.

[3] Ryan Moshell, Comment, . . . *And Then There Was One: The Outlook for a Self-Regulatory United States Amidst a Global Trend Toward Comprehensive Data Protection*, 37 TEX. TECH. L. REV. 357, 362 (2006) (citing Anna E. Shimanek, Note, *Do You Want Milk With Those Cookies?: Complying With the Safe Harbor Privacy Principles*, 26 J. CORP. L. 455, 457 (2001)).

[4] *ChoicePoint Settles Data Security Case*, N.Y. TIMES, June 1, 2007, at C2; *see also ChoicePoint 1Q Profit Tumbles on Charges*, BOSTON GLOBE, Apr. 25, 2008, *available at* http://www.boston.com/business/articles/2008/04/25/choicepoint_1q_profit_tumbles_on_charges/ (noting that ChoicePoint's total revenue in the first quarter of 2007 rose 4.9 percent to $256.4 million from $244.5 million in the year-ago period).

behaviors and shopping habits have been turned into commodities with little concern about the potential for abuse.

Consumers lose a large element of their privacy when they use services as commonplace as Gmail and Amazon.com. Google's Gmail may retain its users' emails and personal contacts, even if the users delete that data.[5] When a user clicks a link on Amazon.com, its database retains not only the information one might expect—things like 'Wish Lists,' reviews, and records of what you purchased—but also:

> the Internet protocol (IP) address used to connect [ones] computer to the Internet; login; e-mail address; password; computer and connection information such as browser type, version, and time zone setting, browser plug-in types and versions, operating system, and platform; purchase history . . . ; the full Uniform Resource Locator (URL) clickstream to, through, and from [the company's] Web site, including date and time; cookie number; products [one] viewed or searched for; [ones] Auction history; and the phone number . . . used to call [the company's] 800 number.[6]

Each time a user signs up for an account, types his or her address, social security number, or pet's name, pays with a credit card or clicks an Internet advertisement, the user incrementally adds to his or her profile and global data footprint. This data trail, combined with other information such as DNA sequences, fingerprints, passport biometrics, and credit card and banking history can create a comprehensive profile of every aspect of an individual's life. Even in the offline world, individuals generate personally identifiable data – ranging from surveillance videos, credit card purchases, 'shopping club' cards, motor vehicle records, and library records. Additionally, computer-biometric methods are on the rise. "[E]merging technologies for identification of individuals include face recognition systems, hand geometry (palm prints), voice

[5] *See* Gmail Privacy Notice (Sept. 12, 2008), http://mail.google.com/mail/help/privacy.html ("Residual copies of deleted messages and accounts may take up to 60 days to be deleted from our active servers and may remain in our offline backup systems.").

[6] Amazon.com, Privacy Notice (Feb. 13, 2010), http://www.amazon.com/gp/help/customer/display.html?ie=UTF8&nodeId=468496#examples. Amazon "may also use browser data such as cookies, Flash cookies (also known as Flash Local Shared Objects), or similar data on certain parts of our Web site [sic] for fraud prevention and other purposes[, and d]uring some visits [it] may use software tools such as JavaScript to measure and collect session information, including page response times, download errors, length of visits to certain pages, page interaction information (such as scrolling, clicks, and mouse-overs), and methods used to browse away from the page."

recognition systems, gait recognition (how a person moves), and DNA databases."[7]

Unfortunately, and in large part due to the current lack of a comprehensive United States data protection law, there have been a number of breaches of databases that contain personal information. Some of the highly publicized data breaches in the past few years—affecting such companies as ChoicePoint,[8] T.J. Maxx,[9] Discount Shoe Warehouse,[10] as well as many universities[11]—have been well documented. These breaches will occur with increasing frequency as the amount of stored personal information proliferates and legislatures continue to forestall enacting laws compelling collectors to safeguard this data. Experts say the general rule here is "once information is 'out,' forget about maintaining exclusive control over it."[12]

This disturbing mix of mass-storage with little oversight results from the current ad-hoc patchwork of federal and state legislation, as well as market failure with respect to privacy protections. In 2008, the Identity Theft Resource Center documented "656 reported breaches at the end of 2008, reflecting an increase of forty-seven percent over last year's total of 446."[13] Each year the breaches become more frequent,

---

[7] *Privacy and Cybercrime Enforcement Act of 2007: Hearing on HR 4175 Before the Subcomm. On Crime, Terrorism, and Homeland Security*, 110th Cong. 93 (2007) [hereinafter *Coney*] (statement of Lillie Coney, Assoc. Dir., EPIC).

[8] *See* Press Release, Federal Trade Commission, ChoicePoint Settles Data Security Breach Charges; to Pay $10 Million in Civil Penalties, $5 Million for Consumer Redress, Jan. 26, 2006, *available at* http://www.ftc.gov/opa/2006/01/choicepoint.shtm.

[9] *See* Brad Stone & Eric Dash, *TJX Says Customer Data Was Stolen*, N.Y. TIMES, Jan. 18, 2007, at C11.

[10] *See* Eric Dash, *Main Street in the Crosshairs*, N.Y. TIMES, Jul. 26, 2005, at C1.

[11] Susan Kinzie, *Stolen Hard Drive Had Personal Data*, WASH. POST, Jan. 30, 2008, at B3 ("A computer hard drive that was reported stolen from a Georgetown University office Jan. 3 contained identifying information about 38,000 current and former students and employees . . . ."); Susan Kinzie, *U-Va. Officials Announce Database Breach*, WASH. POST, Jun. 9, 2007, at B5 (reporting that for about 54 days, an unauthorized hacker broke into a University of Virginia database that included Social Security numbers and other personal information about faculty members); Brad Stone, *800,000 Affected by Data Breach, U.C.L.A. Says*, N.Y. TIMES, Dec. 13, 2006, at A28 (reporting that hackers exposed the private information of 800,000 current and former faculty, staff and students).

[12] Jerry Kang & Benedikt Buchner, *Privacy in Atlantis*, 18 HARV. J.L. & TECH. 229, 242 (2004).

[13] IDENTITY THEFT RESOURCE CTR., SECURITY BREACHES 2008, *available at* http://www.idtheftcenter.org/artman2/publish/lib_survey/Breaches_2008.shtml (last visited Oct. 2, 2009); *see also* IDENTITY THEFT RESOURCE CTR., 2008 DATA BREACH STATS, *available at* http://www.idtheftcenter.org/artman2/uploads/1/ITRC_Breach_Stats_Report_2008_final_1.pdf (last visited Oct. 2, 2009). Based on ITRC's categorization, the 2008 breaches break down as follows: 52.5% in the banking, credit, and financial sectors, 20.5% from medical and healthcare providers,16.5% from general business, 8.3%

contain more data, and make available to criminals more individuals' personal information, as such information is sold to businesses and aggregated by brokers such as ChoicePoint. Today the most profitable commodity is the data surrounding our very existences.

Whoever dismisses the dangers of the increased availability of personal information with the smug confidence of having "nothing to hide" misses the point. Security technologist and author Bruce Schneier addresses such an attitude as follows:

> Cardinal Richelieu understood the value of surveillance when he famously said, 'If one would give me six lines written by the hand of the most honest man, I would find something in them to have him hanged.' Watch someone long enough and you'll find something to arrest – or just blackmail – with. Privacy is important because without it, surveillance information will be abused: to peep, to sell to marketers and to spy on political enemies – whoever they happen to be at the time.[14]

We are all bound by the decisions, health problems, mistakes, and purchases of our pasts, all of which can lead to loss of employment, higher insurance premiums, and other problems. Lillie Coney, Associate Director of the Electronic Privacy Information Center, argues that lives "are judged by the sum total of personal information that is collected, stored, maintained, and shared among commercial data holders."[15] The premise of this Article is that comprehensive federal legislation to regulate privacy is the best way to get businesses, hospitals, and schools to take data privacy protection seriously: "Regulation—SOX, HIPPA, GLB, the credit-card industry's PCI, the various disclosure laws, the European Data Protection Act, whatever—has been the best stick the industry has found to beat companies over the head with [because] regulation forces companies to take security more seriously."[16]

---

from government and military sources, and 2.3% from educational institutions. These breaches affected 219,446,406 people. *Id.*

[14] Bruce Schneier, *The Eternal Value of Privacy*, WIRED, May 18, 2006, http://www.wired.com/politics/security/commentary/securitymatters/2006/05/70886.

[15] Coney, *supra* note 7, at 9.

[16] Michael S. Mimoso, *Bruce Schneier Reflects on a Decade of Security Trends*, SEARCHSECURITY.COM, Jan. 1, 2008, http://www.searchsecurity.com.au/topics/article.asp?DocID=1283751&NodeID=303585.

Indeed, the time has come for the United States to join the "swing toward centralized data protection schemes."[17] Much in the same way the United States has stubbornly refused to adopt the metric system, the United States is becoming an outsider in the area of privacy legislation: "Without legislation that provides a solid support structure for what little government data-protection authority exists, the United States suffers from a general lack of enforcement that stems from industry disregard for voluntary data-protection concepts."[18]

As long as the costs to the company remain external (in that the user expends his or her time and money to clear his or her identity after it has been stolen), companies will be content with the status quo. These costs will have to become internal costs through the 'sticks' of criminal liability or civil litigation and damages in order to make companies take serious measures to guard personal information data.

This Article proceeds in six main parts. Part II discusses portions of the European Union's Directive on Data Protection[19] and argues that a similar law, akin to the EU Directive, would benefit the United States. An exhaustive in-depth discussion of the EU Directive is beyond the scope of this Article, but I will summarize the key points as they pertain to a possible United States data protection law. Part III explores the reasons why existing United States law, such as property, contract and tort law, is not sufficient to protect privacy interests. Part IV shows why comprehensive data protection legislation would be a force for good in the face of the obvious United States market failure with respect to privacy protections. Part V describes why creating national privacy legislation would not be cumbersome and quickly outdated. Part VI discusses key points a comprehensive United States policy should include.

II. THE EU DIRECTIVE 95/46/EC AND THE CURRENT STATE OF LEGISLATION IN THE UNITED STATES

Perhaps unsurprisingly, the United States and the nations of the European Union have different theoretical and practical positions on data privacy. These viewpoints diverge, perhaps

[17] Moshell, *supra* note 3, at 388 (arguing through a comparative analysis of worldwide data protection standards that most of the world is moving toward centralized data protection scheme and that, as a result, the United States is alienating itself from the emerging active roles of other countries by adhering to its existing data-protection regime).

[18] *Id*. at 384.

[19] *See* Council Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 821) [hereinafter EU Directive].

most importantly, on the issue of the appropriate level of government intervention in the regulation of personal information use by the private sector:

> The United States uses a sectoral approach that relies on a mix of legislation, regulation, and self-regulation. The European Union, however, relies on comprehensive legislation that, for example, requires creation of government data protection agencies, registration of databases with those agencies, and in some instances prior approval before personal data processing may begin.[20]

A. The European Union

The European Union "adopted the Data Privacy Directive on October 24, 1995 … [which] went into effect on October 25, 1998."[21] The overarching goal of the Directive is to "protect the fundamental rights and freedoms of natural persons and in particular their right to privacy."[22] It "was passed in response to growing concerns about the improper use, collection, and dissemination of personal information,"[23] and was intended to "set forth a general framework for European data-protection law with the intent of providing a 'harmonized floor of protection' for all EU member states."[24]

The EU Directive prescribes specific requirements for the handling, or "processing," of personal data, defined as "any information relating to an identified or identifiable natural person."[25] Thus, an "identifiable person" (the "data subject" of the personal data) is "one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity."[26]

---

[20] U.S. DEP'T OF COMMERCE, SAFE HARBOR OVERVIEW, http://www.export.gov/safeharbor/eg_main_018236.asp (last visited Oct. 2, 2009).

[21] Robert R. Schriver, Note, *You Cheated, You Lied: The Safe Harbor Agreement and Its Enforcement by the Federal Trade Commission*, 70 FORDHAM L. REV. 2777, 2784 (2002).

[22] EU Directive, *supra* note 19, at ch. I., art. 1, ¶ 1.

[23] Schriver, *supra* note 21, at 2778.

[24] Moshell, *supra* note 3, at 368. *But cf.* The European Commission, Status of Implementation of Directive 95/46 on the Protection of Individuals with regard to the Processing of Personal Data, http://ec.europa.eu/justice_home/fsj/privacy/law/implementation_en.htm (last visited Oct. 8, 2009). Each Member State enacts its own legislation, which can be more stringent than the Directive, which has resulted in varied levels of data protection around the EU. *Id.*

[25] EU Directive, *supra* note 19, at ch. I, art. 2(a).

[26] *Id*.

The EU Directive specifies that an individual's personal information may only be collected for "specified, explicit and legitimate purposes."[27] Information collected is only kept in identifiable form for as long as it is "necessary for the purposes for which the data were collected or for which they are further processed."[28] Data must be accurate. If such information becomes "inaccurate or incomplete", the information must be "erased or rectified."[29] Thus, "[u]nder the Directive, in the broadest terms, personal data must not be processed without the consent of the data subject unless that processing is necessary for performance of a contract with the data subject or a specific exception applies."[30]

The eight basic principles established by the directive are "purpose limitation, data quality, data security, sensitive data protection, transparency, data transfer, independent oversight, and individual redress."[31] These principles require that personal information is only collected and used for specific purposes and such information is stored for "no longer than necessary for the purposes for which the data were collected or for which they are further processed."[32] When data is transmitted and processed, appropriate safeguards must be taken.[33] Sensitive personal data relating to religion, sexual preference, ethnic origin, health, and so forth, is generally prohibited.[34] This means that sensitive data cannot be "processed."[35]

There are exceptions to this rule. For example, sensitive data may be processed "for the purposes of preventive medicine,"[36] or "for the purposes of carrying out the obligations and specific rights of the controller in the field of employment law."[37] Additionally, such data may be processed if "it is authorized by national law providing for adequate safeguards"[38] and if "the processing relates to data which are manifestly made public by the data subject"[39] or "is necessary for the establishment,

---

[27] *Id*. at ch. II, § I, art. 6(1)(b).
[28] *Id*. at ch. II, § I, art. 6(1)(e).
[29] *Id*. ch. II, § I, art. 6(d).
[30] Moshell, *supra* note 3, at 369.
[31] *Id*. at 368.
[32] EU Directive, *supra* note 19, at ch. II, § I, art. 6(e).
[33] *See Id*. at ch. II, § I, art. 6(1)(b).
[34] *Id.* at ch. II, § III, art. 8(1).
[35] *Id.* at ch. I, art. 2(b). "Processing" is defined as "collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction." *Id.*
[36] *Id.* at ch. II, § III, art. 8(3).
[37] EU Directive, *supra* note 19, at ch. II, § III, art. 8(2)(a).
[38] *Id.*
[39] *Id.* at ch. II, § III, art. 8(2)(e).

exercise or defence [sic] of legal claims."[40] In certain Member States, sensitive data—even with an individual's consent—cannot be transferred.[41]

However, the EU Directive allows Member States to decide whether to prohibit the voluntary disclosure of sensitive data. Article 8(1) of the EU Directive states: "Member States shall prohibit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life."[42] However, according to Article 8(2), this prohibition does not apply where "the data subject has given his explicit consent to the processing of those data, except where the laws of the Member State provide that the prohibition referred to in paragraph I *may not be waived by the data subject giving his consent*."[43]

The overarching goal of transparency is to ensure openness and understanding regarding the collection methods, the intended use of data, and the identification of the data collector. The data transfer provisions of the EU Directive limit the unauthorized transmission of personal data to third parties without the data subject's consent.[44] The creation of an independent oversight board provides an autonomous authority with the ability to investigate data practices and enforce sanctions against violators. Lastly, the individual redress policy allows individuals to view their collected personal information to ensure its accuracy. If entities or data collectors violate any practices, individuals may pursue legal action against them.

B. United States

1. Legislation

In the 1990s, while the European Union was creating a comprehensive data directive for its member states, the United States was setting its own course for data privacy protection. Around the same time that "Europe and other governments were developing new legal regimes to protect privacy," the United States was "pursuing legal and technical measures to enable surveillance."[45] Instead of creating a comprehensive data protection scheme, "the United States has [so far] protected

---

[40] *Id*.
[41] *Id*. at ch. II, § III, art. 8(3).
[42] EU Directive, *supra* note 19, at ch. II, § III, art. 8(1).
[43] *Id*. at ch. II, § III, art. 8(2) (emphasis added).
[44] *Id.* at ch. II, §II, art. 7.
[45] Marc Rotenberg, *Fair Information Practices and the Architecture of Privacy (What Larry Doesn't Get)*, 2001 STAN. TECH. L. REV. 1, ¶ 117 (2001), http://stlr.stanford.edu/pdf/rotenberg-fair-info-practices.pdf.

personal data only in an ad hoc, sectoral manner, either regulating specific industries or specific types of information and then, only in reaction to specific data protection problems."[46] The reasons for this limited protection "have ranged from First Amendment concerns and the free flow of information to the promotion of commerce and wealth, to 'a healthy distrust for governmental solutions.'"[47]

Instead of passing a comprehensive data protection law, "the United States government turned to the private sector for self-regulatory measures that offered little in the way of actual privacy protections."[48]

The United States, however, is not totally bereft of privacy legislation; it enacts such legislation to regulate specific industries every few years.[49] This per-industry legislating has

---

[46] Edward C. Harris, *Personal Data Privacy Tradeoffs and How a Swedish Church Lady, Austrian Public Radio Employees, and Transatlantic Air Carriers Show That Europe Does Not Have the Answers*, 22 AM. U. INT'L L. REV. 745, 746 (2007).

[47] Schriver, *supra* note 21, at 2779 (quoting James M. Assey, Jr. & Demetrios A. Eleftheriou, *The EU-U.S. Privacy Safe Harbor: Smooth Sailing or Troubled Waters?*, 9 COMM LAW CONSPECTUS 145, 150 (2001)).

[48] Rotenberg, *supra* note 45, ¶ 117.

[49] *See, e.g.*, Computer Matching and Privacy Protection Act of 1988, 5 U.S.C. §552a (2006) (governing the safeguarding of privacy through four procedural and substantive rights in personal data) (amending Privacy Act of 1974); Right to Financial Privacy Act of 1978, 12 U.S.C. §§ 3401-3422 (2006) (governing the handling of financial information held by financial institutions); Fair Credit Reporting Act of 1970, 15 U.S.C. §§1681-1681x (2006) (governing the use of credit information in consumer credit decisions); Fair Debt Collection Practices Act, 15 U.S.C. §1692-1692p (governing collection of consumer debts, while promoting fair debt collection and providing consumers with an avenue for disputing and obtaining validation of debt information); Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501-6506 (2006) (governing the online collection of personal information from children under the age of 13); Identity Theft Penalty Enhancement Act of 2004, 18 U.S.C. §1028 (2006) (establishing aggravated identity theft as a new federal crime); Video Privacy Protection Act of 1998, 18 U.S.C. § 2710 (2006) (governing the privacy of video tape rental, purchase, and delivery information); Driver's Privacy Protection Act of 1994, 18 U.S.C. §2721-2725 (2006) (governing the public disclosure of personal information contained in state department of motor vehicle records); Family Educational Rights and Privacy Act of 1974, 20 U.S.C. §1232g (governing the privacy of student education records); Privacy Protection Act of 1980, 42 U.S.C. §§2000aa-2000aa-12 (2006) (governing government access to journalist's work product); Telephone Consumer Protection Act of 1991, 47 U.S.C. §227 (2006) (governing telemarketers' use of certain consumer information); Cable Communications Policy Act of 1984, 47 U.S.C. §551 (2006) (governing cable television providers' use of customer information); Gramm-Leach-Bliley Act of 1999, Pub. L. No 106-102, 113 Stat. 1338 (1999) (codified with some differences in language at 15 U.S.C. § 6801 (2006)) (governing the handling of financial data by financial institutions); Fair and Accurate Credit Transactions Act of 2003, Pub. L. No. 108-159, 117 Stat. 1952 (2003) (codified with some differences in language at 15 U.S.C. §1681 (2006)) (amending the Fair Credit Reporting Act); Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191 §262 (codified with some differences in language at 42 U.S.C. §1301 (2006)) (governing the use of personal medical data by health professionals and health insurance providers); s*ee also*, Better Business Bureau, *A Review of Federal and State Privacy Laws*, *available*

resulted in the current state of patchwork regulation. There has been no federal consensus as to whether a comprehensive data structure would be a good for the United States, and without this consensus, Congress must step in every few years to resolve new privacy controversies:

> Congress, state legislatures, and oversight agencies such as the Federal Trade Commission were reluctant to enact broad-based privacy rules, perceiving a lack of consensus on generally accepted privacy principles and fearing the erosion of societal benefits brought about by new technologies and the free flow of information. To this day, information privacy in the United States relies heavily on individuals guarding the integrity of their data records and protecting personal information from unintended use.[50]

This piecemeal legislation by the federal government and the states, combined with market-driven approaches by businesses, has led to gaps, overlaps, lack of clarity, and inconsistencies. The end result has been the loss of personal privacy:

> The increasing importance of international data transfer in the global economy, when combined with a global trend toward comprehensive data protection, highlights the necessity of a United States data-protection position that contributes to, rather than detracts from, global stability. To that end, the United States must follow the example of nations that have established moderate variants of the EU's comprehensive data-protection framework and establish a regime that moves toward the middle of the spectrum.[51]

The EU Directive is already playing an important role in the United States economy as it restricts the flow of data to third countries, which lack data protection laws that do not meet the standards of the EU Directive. "Third countries" in this sense are countries outside the European Union. The EU Directive states that personal data may be transferred to a "third country" if "the third country in question ensures an adequate level of

---

at http://www.bbbonline.org/UnderstandingPrivacy/library/fed_statePrivLaws.pdf (last visited Oct. 3, 2009).

[50] James P. Nehf, *Incomparability and the Passive Virtues of Ad Hoc Privacy Policy*, 76 U. COLO. L. REV. 1, 2 (2005) [hereinafter *Incomparability*] (citing James P. Nehf, *Recognizing the Societal Value in Information Privacy*, 78 WASH. L. REV. 1, 48-58 (2003) [hereinafter *Recognizing the Societal Value*]).

[51] Moshell, *supra* note 3, at 359-360.

protection,"[52] and such adequacy "shall be assessed in the light of all the circumstances surrounding a data transfer."[53] These circumstances include "consideration . . . [of] the nature of the data, the purpose and duration of the proposed processing operation . . . , the country of origin and the country of final destination, the rules of law . . . in force in the county . . . [,] and the professional rules and security measures which are complied within that country."[54]

When the EU Directive was first discussed, there were concerns that trade with the United States would come to a halt as a result of this restriction. The United States "struck a political compromise with the EU to ease concerns expressed by both sides regarding potential disruptions in trade relations."[55] This compromise came to be known as the Safe Harbor. The Safe Harbor "does not bind U.S. states to embrace comprehensive privacy standards."[56] Yet "on the corporate level the Safe Harbor replaces the sectoral approach by requiring company compliance with specific principles of 'adequate protections' regarding the collection and use of personal data."[57] The Safe Harbor was entered into in July 2000.[58] Thus, "[t]he influence of the EU Directive upon U.S. privacy law is noteworthy in that it represents a situation in which a comprehensive regime, with strict standards, is finding its way into a less strict, sectoral regime."[59] In the past few years various bills have been proposed in Congress—both comprehensively and sectorally—that draw on EU Directive standards.[60] Additionally, numerous proposed and enacted state

---

[52] EU Directive, *supra* note 19, at ch. IV, art. 25(1).

[53] *Id.* at ch. IV, art. 25(2).

[54] *Id.*

[55] Kamaal Zaidi, Comment, *Harmonizing U.S.-EU Online Privacy Laws: Toward a U.S. Comprehensive Regime for the Protection of Personal Data*, 12 MICH. ST. J. INT'L L. 169, 176 (2003).

[56] *Id.*

[57] *Id.*; *see also Google Bosses on Trial in Italy*, BBC NEWS, Sept. 30, 2009, *available at* http://news.bbc.co.uk/2/hi/technology/8282293.stm. Because of the difference between United States and European Union laws, Google executives are facing possible jail time in Italy. The case revolves around a 2006 Google Video showing "a teenager with Down's syndrome being bullied by four students in front of more than a dozen others." *Id.* The Italian prosecutors argue that "Google broke Italian privacy law by not preventing the content from being uploaded without the consent of all parties involved." *Id.* This case illustrates the challenges companies face to comply with different international legal rules.

[58] U.S. Dep't of Commerce, *Safe Harbor Overview*, *supra* note 20.

[59] Zaidi, *supra* note 55, at 175.

[60] *See* Personal Data Privacy and Security Act of 2009, S.1490, 111th Cong. (2009) (establishing "standards for developing an implementing safeguards to protect the security of sensitive personally identifiable information," and creating civil penalties for violations of the standards). Even more importantly, this bill would authorize "the Attorney General and state attorneys general to bring civil actions against business entities for violations of this Act" and would establish "in the Federal

bills impose more stringent requirements on companies when they handle personally identifiable information.[61] In fact, "specific elements of privacy protections found in the Directive and the Safe Harbor are finding their ways into state privacy laws."[62]

2. The FTC

Most nations have a Data Protection Board that enforces and monitors its country's data protection legislation to ensure it functions properly.[63] The United States, however, has no such

---

Trade Commission an Office of Federal Identity Protection." *See also* Data Accountability and Trust Act, H.R. 2221, 111th Cong. (2009) (establishing national standards for data breaches notifications, regulate information brokers, and requires companies to adopt security policies.); Privacy and Cybercrime Enforcement Act of 2007, H.R. 4175, 110th Cong. (2007) (amending the federal criminal code provisions relating to computer fraud and unauthorized access to computers, creating criminal penalties if there is an intentional failure to provide notice of security breaches involving personally identifiable information, authorizing additional appropriations for investigating and prosecuting criminal activity involving computers, and authorizing the Attorney General and state attorneys general to bring civil actions and obtain injunctive relief for violations of federal laws relating to data security); Internet Stopping Adults Facilitating the Exploitation of Today's Youth Act of 2007, H.R. 837, 110th Cong. (2007) (requiring all Internet service providers to track their customers' online activities to aid police and imposing fines and prison terms of up to one year upon anyone who fails to store that information); Eliminate Warehousing of Consumer Internet Data Act of 2006, H.R. 4731, 109th Cong. (2006) (covering the Internet, cable operators and any company that gathers personal information that can identify individual consumers and acknowledging that "Internet search engines provide an extraordinary service, but the preservation of that service does not rely on a bottomless, timeless database that can do great damage despite good intentions."); Identity Theft Protection Act of 2006, H.R. 5482, 109th Cong. (2006) (amending the Fair Credit Reporting Act to provide individuals the ability to control access to their credit reports, and "for other purposes"); Personal Data Privacy and Security Act of 2005, S.1789, 109th Cong. (2005) (establishing mechanisms "to prevent and mitigate identity theft, to ensure privacy, to provide notice of security breaches, and to enhance criminal penalties, law enforcement assistance, and other protections against security breaches, fraudulent access, and misuse of personally identifiable information"); Identity Theft Protection Act, S. 1408, 109th Cong. (2005) (enhancing "data protection and safeguards and requiring data breach notification in order to further prevent identity theft"); Notification of Risk to Personal Data Act, S. 715, 109th Cong. (2005) (requiring Federal agencies and persons engaged in interstate commerce while in possession of electronic data containing personal information to disclose any unauthorized acquisition of such information).

[61] *See* Holly K. Towle, *Newsstand: Proliferation of Information Security Breach Notification Statutes*, Jul. 21, 2005, http://www.klgates.com/newsstand/Detail.aspx?publication=3282 (explaining the requirements of companies in California, Georgia, Montana, and North Dakota when they deal with personally identifiable information).

[62] Zaidi, *supra* note 55, at 195.

[63] *See generally*, Electronic Privacy Information Center and Privacy International, *Privacy and Human Rights: An International Survey of Privacy Laws and Developments* (2006), http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-559552&als[theme]=Privacy%20and%20Human%20Rights%202004. In Germany, "[t]he Federal Commissioner for Data Protection and Freedom of Information (Bundesbeauftragter für den Datenschutz) is an independent federal agency that

board. Instead, "[i]n a nation where the track record for data privacy protections is "spotty at best," the Federal Trade Commission ("FTC") has become the United States' beleaguered leader in advocating data privacy advances."[64] "Data protection must therefore compete with the entirety of U.S. commerce for FTC priority."[65]

The FTC's responsibility is to monitor all domestic United States commerce—and some foreign commerce—within the United States for any uses of unfair means of competition or deceptive trade practices.[66] The FTC does not have any specific authority over data protection per se.[67] Instead, "[t]he FTC's mission is to protect consumers from fraudulent or deceptive claims that mislead consumers, and from harmful business practices that undermine the competitive process."[68] It protects against unfair or deceptive acts and practices via Section 5 of the Federal Trade Commission Act ("FTCA"), which proscribes "unfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce."[69] The FTC has used this power to enforce privacy policies.

As discussed above, most businesses, both on- and off-line, collect personal information as a routine practice—ostensibly under the auspices of their privacy policies. However, "there is no law requiring privacy policies or prescribing their content." Consequently, privacy policies can offer little or no privacy protection, and if a privacy policy is breached the individual has little practical recourse.[70]

The FTC is currently serving in a reactive instead of a proactive manner because it must "wait until the organization misleads the public as to those practices."[71] Incidents of

---

supervises the Federal Data Protection Act as well as the Federal Freedom of Information Act"; in Norway, "enforcement of the Personal Data Act of 2000 is overseen by The Data Inspectorate (Datatilsynet)" which "is placed under the administrative wings of the Ministry of Labor and Government Administration, but is otherwise expected to function completely independently of government or private sector bodies"; in Estonia, "[t]he Data Protection Inspectorate is the supervisory authority for the Personal Data Protection Act, the Databases Act and the Public Information Act"; in Sweden, "compliance with the Swedish Personal Data Act or personuppgiftslagen is monitored by the independent Data Inspection Board, Datainspektionen. *Id.*

[64] Moshell, *supra* note 3, at 381.

[65] *Id*.

[66] *Id*. at 425.

[67] *See Id.*

[68] FTC, *Welcome to the Office of Policy Planning*, http://ftc.gov/opp/index.shtml (last visited June 14, 2007).

[69] 15 U.S.C. § 45(a)(1) (2006).

[70] Nehf, *Incomparability*, *supra* note 50, at 15.

[71] Moshell, *supra* note 3, at 429.

misleading the public fall under the FTC's milieu, and the FTC may act if and only if a company practices "unfair or deceptive" practices pursuant to the FTCA.[72] Absent "comprehensive legislation establishing fair information practice principles in the rule of law, the FTC cannot prevent data collection and distribution in any scenario unless the collector has posted a privacy policy and then failed to operate under that policy."[73]

Furthermore, private parties cannot bring an action for themselves: "The FTCA mandates that only the FTC can initiate and maintain court proceedings related to the matter."[74]

Even if the FTC acts, what usually happens in the best case is that the company under investigation settles with the FTC and the "organization agrees to discontinue practices that violate the FTC's Fair Information Practice Principles."[75] However, "the commission [usually] must settle for pursuing an order prohibiting the misrepresentation made by the organization."[76] While there have been recent cases in which the FTC has required companies to disgorge assets in response to their transgressions, this is the exception rather than the rule.[77]

The FTC can obtain injunctive remedies. In addition, "[f]or some violations there may be a private remedy under state deceptive-practices statutes, but many require proof of actual injury, prohibit class actions, or place significant procedural obstacles in the way of consumer redress."[78]

It does not appear that the FTC will be granted any specific authority over data protection, nor will it advocate for comprehensive privacy legislation. The FTC "has developed information practice principles, encouraged self-regulatory measures in the private sector, and, except for a period during

---

[72] 15 U.S.C. § 45 (2006).

[73] Moshell, *supra* note 3, at 383.

[74] *Id.* at 425.

[75] *Id.* at 429.

[76] *Id.*

[77] *See, e.g.*, *In Re* DSW Inc., FTC Docket No. C-4157 (Mar. 7, 2006), *available at* http://www.ftc.gov/os/caselist/0523096/0523096c4157DSWComplaint.pdf (ordering DSW to establish and maintain a comprehensive information security program that includes administrative, technical, and physical safeguards and requiring DSW to obtain, every two years for the next 20 years, an audit from a qualified, independent, third-party professional to assure that its security program meets the standards of the order); Consent Order, U.S. v. ChoicePoint Inc., FTC File No. 052-3069 (Feb. 10, 2006) *available at* http://www.ftc.gov/os/caselist/choicepoint/0523069stip.pdf Because of a breach resulting in compromised financial records of more than 163,000 ChoicePoint customers, the FTC settled with ChoicePoint, requiring the company to pay $10 million in civil penalties and provide $5 million for consumer redress. *Id.*; *see also In re* Liberty Companies, Inc., FTC Docket No. C-3891 (May 6, 1999) *available at* http://www.ftc.gov/os/1999/05/lbtyord.htm (ordering Liberty Financial Companies to post a clear and prominent privacy statement).

[78] Nehf, *Incomparability*, *supra* note 50, at 15-16.

2000 when it advocated codification of information principles, stood as an opponent to comprehensive data-protection legislation."[79]

3. Technological Solutions

The United States relies heavily on the individual to enact technological solutions to protect his or her personally identifiable information. An in-depth discussion of every possible self-help method is beyond the scope of this Article. However, I will briefly discuss P3P, privacy seals and user cookie management as examples. Because of the widespread commoditization of personally identifiable information, "technological developments continually increase data collection and decrease our ability to impede the process, [and this] makes privacy protection even more difficult for people who might be interested in curbing data collection practices by policing their information in the marketplace."[80] In addition, technological solutions "offer no privacy protection to consumers with regard to offline data collection."[81]

The World Wide Web Consortium (W3C) designed P3P, or Platform for Privacy Preferences, in order to make website practices "explicit and thus open them to public scrutiny."[82] P3P allows a user to set a data privacy threshold and "to automate decision-making based on these practices [sic] when appropriate."[83] Internet users, therefore, "need not read the privacy policies at every site they visit."[84] If a website has a privacy policy in conflict with the user's data privacy threshold, then the user is alerted by a warning.[85] Such warnings "may take different forms—for example pop-up messages that require the user to make a decision, or icons in the corner of the browser window that do not require user action."[86] Critics have been unenthusiastic about P3P partly because "P3P places the onus on computer users to set their privacy preferences, which given the limited technical knowledge and awareness of most users, is bound to limit the impact of P3P."[87] In addition, there is a lack of enforcement with P3P self-help because "[n]o law or

---

[79] Moshell, *supra* note 3, at 381.

[80] Nehf, *Incomparability*, *supra* note 50, at 27.

[81] McClurg, *supra* note 1, at 92.

[82] *Platform for Privacy Preferences (P3P) Project*, Nov. 20, 2007, http://www.w3.org/P3P.

[83] *Id.*

[84] *Id*.

[85] *What is P3P and How Does it Work?*, http://p3ptoolbox.org/guide/section2.shtml (last visited Oct. 11, 2009).

[86] *Id*.

[87] McClurg, *supra* note 1, at 93-94.

regulation requires Web sites to adopt P3P, nor does any enforcement mechanism exist to ensure that P3P-compliant sites actually follow their privacy policies."[88]

In short, P3P protocols "are complex, difficult to implement, and unlikely to enable consumers to protect privacy[,]"[89] and, "while P3P is a step in the right direction, it is by no means a panacea to protecting information privacy."[90]

Another self-help method the market has implemented is the privacy seal program. Two such programs are the TRUSTe and the BBB*Online* Privacy Seal, "[both of] which rate the privacy policies of Web sites, providing sites that post clear privacy protection policies with a seal of approval."[91] These methods are also inadequate, however, in part because:

> At present, market incentives do not push trust mark licensors to impose rigorous privacy policies on their licensees. While a licensor will insist on a minimally acceptable privacy standard to make its mark appear to have value, insistence on rigorous standards is likely to drive away licensees who prefer laxer standards. What people need is a signal for determining whether a trust mark itself is a meaningful signal. Without mandatory privacy standards to ensure that a mark is worth something – for example, minimum requirements for displaying a privacy "seal of approval" – signals will remain ineffective bridges of the information gap.[92]

Another option individuals have to protect their personally identifiable information online is to disable cookies in their Internet browser. Cookies are "small files that Web sites put on your computer disk drive when [one] first visit[s]."[93] Cookies store user information such as preferences, user names, personalized pages, and passwords, so that when an individual returns to a page with cookies enabled, the user does not need to reenter a password or reset personalized settings. All web browsers have the ability to set, block, or warn users about cookies. This self-help method has one major drawback, however in that "the individual is responsible for coordinating

---

[88] *Id*. at 94.

[89] Rotenberg, *supra* note 45, at 76.

[90] McClurg, *supra* note 1, at 95.

[91] Robert W. Hahn & Anne Layne-Farrar, *The Benefits and Costs of Online Privacy Legislation*, 54 ADMIN. L. REV. 85, 110 (2002).

[92] Nehf, *Incomparability*, *supra* note 50, at 25 (footnote omitted).

[93] Microsoft, *What is a cookie?*, http://www.microsoft.com/protect/terms/cookie.aspx (last visited Oct. 11, 2009).

all the different aspects of her privacy protection."[94] Despite the public being generally informed about private information collection methods on the Internet, and the fact that in 2007 there was "a huge surge in public anxiety over information security,"[95] people are still unaware of how best to protect themselves. A recent survey of Internet users in the United States "revealed that although Americans are aware that their Internet behavior is subject to commercial monitoring, less than half of [them] know what a cookie is, and even fewer know how to take the short, simple steps to set their web browsers to prevent the placement of cookies."[96] In addition, personally identifiable information is increasingly gathered in other ways, such as browser plug-in vulnerabilities, phishing, and tracking done at the Internet Service Provider level.[97] Thus, even a diligent person who monitors cookie files may not be protected. Moreover, for some websites, cookie usage is mandatory. If the cookies are not enabled, the user cannot use the company's site.

III. WHY CONTRACT, TORT, AND PROPERTY LAW DOES NOT PROTECT PRIVACY

Critics of a comprehensive data protection law often argue that there is no need for special private data legislation because there are common law standards in place—contract, tort, and property law—for Internet users to redress any problems that arise. However, these standards fail to protect users' private data. The chief reason for this failure is the fact that consumers do not always know when their data privacy has been breached until it is too late:

> To a large extent, we are operating in a fog when attempting to analyze the privacy implications of consumer data profiling, because so little is

---

[94] Hahn & Layne-Farrar, *supra* note 91, at 136.

[95] Privacy International, *PI Warns That Breaches are Leading to Collapse of Public Trust in IT Systems*, Jan. 20, 2008, http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-559869&als[theme]=Data%20Protection%20and%20Privacy%20Laws.

[96] David A. DeMarco, Note, *Understanding Consumer Information Privacy in the Realm of Internet Commerce: Personhood and Pragmatism, Pop-Tarts and Six-Packs*, 84 TEX. L. REV. 1013, 1019 (2006); *see also* PEW Internet & American Life Project, *PEW Internet Posts*, Nov. 29, 2004, http://www.pewinternet.org/Commentary/2004/November/Surprising-strange-and-wonderful-data.aspx ("56% of online Americans do not know what a cookie is.").

[97] *See* Symantec, SYMANTEC GLOBAL INTERNET SECURITY THREAT REPORT: TRENDS FOR 2008, Volume XIV (April 2009), *available at* http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiv_04-2009.en-us.pdf (discussing increased security threats).

> known about it. The actual analytical processes of data mining are largely impenetrable as a technical matter, and they occur within an industry that does little to facilitate public scrutiny of its practices.[98]

The average Internet user does not typically know what information is being collected about him or her, to whom it is being sold, or how it is being shared. The public, moreover, only hears about a fraction of the data breaches. Thus, "[e]xcept in the rare instance when a privacy breach comes to someone's attention, people will never learn about harms resulting from information collection and misuse."[99] Even if there is a breach of an individual's online privacy, that individual may never become aware of it:

> The vast majority of data collecting—lawful and unlawful—occurs outside public view. Individuals do not know when information collection and sharing has affected them for good or for bad. If a breach of privacy norms results in media exposure, identity theft, or some other cognizable injury, the affected person may learn about it in due course. Less obvious breaches remain hidden for long periods, possibly forever.[100]

Even if an individual knows a breach has occurred, it may be difficult to show that there has been harm from that breach. It is particularly difficult, for example, for an individual to prove that identity theft happened from a particular breach. Identity thieves need only breach a single database to get an individual's name, social security number, credit card number, date of birth, and so forth. If one is a shopper at Discount Shoe Warehouse whose information has been aggregated by ChoicePoint, it may be impossible to determine which breach was at fault. The harm, moreover, may have resulted from a recent data breach or from one that happened years before, where the perpetrator "sat" on the information until it could be used:

> Even with an obvious injury such as identity theft, it may be impossible to learn how the thief obtained the personal information. The thief might have taken Social Security numbers from a university database, driver's

---

[98] McClurg, *supra* note 1, at 98 (footnote omitted).
[99] Nehf, *Incomparability*, *supra* note 50, at 20.
[100] *Id*. at 27-28.

> license numbers from a convenience store scanner, addresses from an insurance company, or credit card numbers from the marketing affiliate of a credit card issuer. Tracing the injury back to the point of origin will often be difficult or impossible.[101]

Thus, if an individual cannot show an individualized harm, it is difficult if not impossible to bring a contract, tort or property claim against an entity, because the individual is missing an integral part of any such claim.

It is unlikely that the enactment of comprehensive data protection legislation would change this problem. Criminal or civil liability only attaches if wrongdoing is found. Thus, the creation in the United States of a Data Protectorate Board, as the EU Directive calls for,[102] would go a long way toward helping the government uncover activities, which contravene the protection legislation.[103]

A. Property

Critics and commentators have suggested creating a property right in personally identifiable information.[104] Despite "numerous creative academic proposals for creating property rights in personal information, current case law provides that while individuals have no property rights in their personal information . . . [,] customer information databases are generally viewed as property of the firms that hold them."[105] In addition, "[c]reating a property right in personal information would amount to the recognition of a new form of intellectual property,

---

[101] *Id*. at 28.

[102] EU Directive, *supra* note 19, at ch. VI, art. 28.

[103] *See, e.g.,* Data Protection Bill of 1991, H.R. 685, 102d Cong (1991) (proposing the creation of a permanent independent board to over data collection and storage); *see also* Robert Gellman, *A Better Way to Approach Privacy Policy in the United States: Establish a Non-Regulatory Privacy Protection Board*, 54 HASTINGS L.J. 1183 (2002); Nehf, *Recognizing the Societal Value*, *supra* note 50, at 68-69; Michael P. Roch, *Filling the Void of Data Protection in the United States: Following the European Example*, 12 SANTA CLARA COMPUTER & HIGH TECH. L.J. 71, 94 (1996).

[104] *See generally* LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 142-63 (1999) (advocating the use of property rights to protect privacy on the Internet); Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193 (1998) (suggesting a statutory solution that is market-driven or property-esque); Richard S. Murphy, *Property Rights in Personal Information: An Economic Defense of Privacy,* 84 GEO. L.J. 2381, 2383-84 (1996) (arguing that "personal information, like all [other] forms of information, is property"); Pamela Samuelson, *Privacy as Intellectual Property?*, 52 STAN. L. REV. 1125, 1126 (2000) (describing consumer data as "a key commercial asset"); Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 HARV. L. REV. 2055, 2095 (2004) (suggesting a five-elemental model for personal information as property).

[105] DeMarco, *supra* note 96, at 1035-36.

but it would be much broader and more ambiguous than currently recognized intellectual property rights."[106]

Granting individuals a property right in their personally identifiable information "would allow the market—made up of buyers, sellers, and competition—to determine the most efficient allocation of this valuable property interest."[107] The existence of such a property right creates the potential for individuals, who feel a company's requests are too intrusive or that they are not getting enough value from their personally identifiable information, to withdraw or "withhold their valuable PII [personally identifiable information] and move to a competitor's product that is less privacy intrusive."[108]

This idea has pitfalls for the individual: "[I]f people do not know what information is being collected, how it could be used, and what harm might result from its collection and use, they have no way of judging how much it is worth (in time, effort, or money) to keep the information private."[109] Additionally, without standards requiring companies to adhere to certain privacy policies, including data aggregators, "[e]ven if asked, the data collector cannot provide enough information to give the individual a meaningful choice."[110] Creating property rights in personally identifiable information would not enable an individual to protect his or her data from being processed and sold. Once a company has a user's personally identifiable information, it is impossible to determine whose hands it may end up in. The difficulties users face in proving which company caused the breach and in proving harm further hinder any attempt to bring a cause of action.

Creating a property right in personally identifiable information raises the question of whether the individual user or the company owns the data. The creation of such a property right is difficult because "[one] can't simply build a fence around [one's] personal information to keep others away from it [and] although [one] notice[s] when somebody has taken away [one's] car, [one] usually [has] no way of knowing when somebody has taken [ones] data."[111] Furthermore, personally identifiable information would be a fundamentally intangible form of property; it could exist in different forms and in different places at the same time. The use of personally

---

[106] McClurg, *supra* note 1, at 92.

[107] Corey A. Ciocchetti, *E-Commerce and Information Privacy: Privacy Policies as Personal Information Protectors*, 44 AM. BUS. L.J. 55, 67 (2007).

[108] *Id.*

[109] Nehf, *Incomparability*, *supra* note 50, at 21.

[110] *Id.* at 22.

[111] Kang & Buchner, *supra* note 12, at 241.

identifiable information by one person does not destroy the property, deprive the individual from using the information, or even prevent others from using it at the same time. This aspect of such information is a primary cause of its excessive proliferation.

B. Tort

Tort law has also been proposed as a way to protect privacy. However, "[C]ourts have long rejected assertions that torts such as intrusion upon seclusion, public disclosure of embarrassing facts, and appropriation of name and likeness ought to be extended to the consumer information privacy context."[112] In addition, as one commentator pointed out, the rejection of tort law is "generally . . . not grounded in philosophical objections to tort law, but in the pragmatic—and largely accurate—view that current tort law simply is not well suited to address information privacy abuses."[113]

Privacy torts seek "to protect individuals from reputational harm[,]"[114] not to "protect an individual's sense of autonomy and to prevent potential losses due to misuse of information."[115] Because of this distinction, privacy torts are ill-equipped to "have much impact on DNA or medical databases since the data are either extracted with consent, or in circumstances such as arrests, where consent is not an issue."[116] In addition, "privacy torts do not protect things in public view on the theory that such things are, by definition, not private."[117] This means public tracking through video surveillance, gait, and voice recognition are not covered by a privacy tort, since these are activities in the public view. Privacy tort law only protects a very narrow class of privacy—a class, which wholly excludes the overarching privacy concerns facing today's online world.

C. Contract

Professor Eugene Volokh has advanced a contract theory for protecting information privacy that would permit consumers to enforce, through breach of contract actions, promises not to reveal information.[118] Volokh "went further and suggested

---

[112] DeMarco, *supra* note 96, at 1036.

[113] McClurg, *supra* note 1, at 97.

[114] Lilia Rode, Comment, *Database Security Breach Notification Statutes: Does Placing the Responsibility on the True Victim Increase Data Security?*, 43 HOUS. L. REV. 1597, 1609 (2007).

[115] *Id.*

[116] A. Michael Froomkin, *The Death of Privacy?*, 52 STAN. L. REV. 1461, 1536 (2000).

[117] *Id.* at 1536.

[118] McClurg, *supra* note 1, at 95.

legislatively imposed default rules that would specify certain transactions as carrying with them an implied promise of confidentiality [that] could be waived by agreeing to a disclaimer that any information was not subject to confidentiality."[119]

However, "for Volokh's contract model to confer meaningful protection for the privacy of consumer data on a widespread basis, legislatures would be required to adopt the theory and enact his proposed implied-contract-of-confidentiality default rules."[120] Convincing the legislature and the courts to implement a contractual right to privacy may prove no less onerous a task than winning the legislature's backing for a more comprehensive data protection scheme.

There is "a dearth" of contract claims of this nature thus far, perhaps because of "the somewhat attenuated relationship between a privacy policy and the typical contractual transaction (i.e. the sale of goods or services) to which such an executory policy might attach."[121] Contract claims are rare, furthermore, because "damages for any such breach, on the individual level, would be prohibitively low, or alternatively, too difficult to quantify."[122] Additionally:

> "It's extremely tough to keep track of personal data in secondary transfers. In other words, even if the info is properly used by the first party, when that party conveys the info to party number two, it's hard for the individuals to verify whether that second party is using the info in accordance with the license, permission, or authorization connected to that data. As a practical matter, once information is 'out,' forget about maintaining exclusive control over it.[123]

The implementation of a comprehensive data protection privacy scheme does not mean that the days of collecting and aggregating personally identifiable information are over. Indeed, "[i]n many situations, consumers have privacy preferences, and, if forced to evaluate privacy terms, consumers would in fact give up some personal information in exchange for added

---

[119] *Id*. at 96.
[120] *Id*. at 96-97.
[121] DeMarco, *supra* note 96, at 1036-37.
[122] *Id*. at 1037.
[123] Kang & Buchner, *supra* note 12, at 241-42.

value."[124] On the other hand, some individuals would "sometimes pay more or give up discounts to have better privacy protection, as many refuse grocery store 'convenience' cards because they do not want their purchasing habits tracked and traded."[125]

In addition, there is a power inequality between businesses and individuals:

> Confronted with a take-it-or-leave-it situation, an individual may lack any practical ability to negotiate privacy terms. After all, the entire point of a form contract is to gain the efficiencies of standardization. Moreover, a company might be the only provider of the goods or services required. In order to obtain a certain benefit, the consumer has no choice but to accept the company's terms even if they require the disclosure of personal information as a necessary prerequisite.[126]

In this type of situation a consumer must accept the terms on which the service is being offered, for "[i]n the marketplace, personal data will be lost in the shuffle, with citizens making bad choices or being coerced into transactions from which they cannot walk away."[127]

IV. WHY LEGISLATION TRUMPS FREE MARKET – MARKET FAILURE

The main argument against a comprehensive data regime in the United States is that sectored legislation and self-regulation are considered the least restrictive methods. In addition, critics claim that "[l]egislative attempts to regulate the specific technological aspects of information privacy are likely to be clumsy and to become quickly outdated."[128] Instead, these critics contend that "letting the market decide [gives] . . . citizens . . . the power to choose 'their optimal mix of privacy' without paternalistic intervention from the state."[129] This theory advances the idea that the market is the most effective way to protect the privacy of Internet users. The market itself, however, has not vindicated this stance. Current American privacy policy

---

[124] James P. Nehf, *Shopping for Privacy Online: Consumer Decision-Making Strategies and the Emerging Market for Information Privacy*, 2005 U. ILL. J.L. TECH. & POL'Y 1, 14 (2005) [hereinafter *Shopping*].

[125] *Id.*

[126] Kang & Buchner, *supra* note 12, at 245.

[127] *Id.* at 244.

[128] McClurg, *supra* note 1, at 91.

[129] Kang & Buchner, *supra* note 12, at 233 (quoting Steven A. Bibas, *A Contractual Approach to Data Privacy*, 17 HARV. J.L. & PUB. POL'Y 591, 611 (1994)).

"reflects what industry is prepared to do rather than what the public wants done."[130]

In reality, "[t]he market incentives are weak . . . and the conditions of market failure are strong"[131] because the United States demands no real accountability for companies that disclose information, and, "[w]ithout accountability, market forces cannot effectively curb harmful behavior."[132] Even media exposure does not provide adequate accountability. There have been "a number of . . . examples of the press uncovering corporate information sharing plans that generated public outrage[,]"[133] and such stories provide "a fast, low cost method for unhappy consumers to protest."[134] However, this oversight is not always effective because breaches are not always disclosed or even reported.

Currently, the only way to bring a claim is through contract or tort as discussed above. The FTC can prosecute businesses, but may only do so if a business acts contrary to its privacy policy. An individual, however, cannot bring a claim on his own behalf.[135]

A. Control

Legislation is needed to give people a certain level of control over their personal data, so that they may dole it out or keep it processed to a minimum as they see fit. However, some personal data is too important to barter away – such as genetic data, biometrics, and health-related data. For this type of information, people should not be able to grant access, such as in the EU Directive art. 8(2). Such a prohibition should not, for example, prevent processing of data when it "is required for the purposes of preventive medicine, medical diagnosis" or when it "is necessary for the establishment, exercise or defence [sic] of legal claims" or "where the data subject is physically or legally incapable of giving his consent."[136] In these exceptional cases, the information should be processed and collected under stricter circumstances and with "suitable safeguards."[137]

---

[130] Rotenberg, *supra* note 45, at ¶ 119.
[131] Nehf, *Incomparability*, *supra* note 50, at 19.
[132] *Id.*, at 27.
[133] Hahn & Layne-Farrar, *supra* note 91, at 108.
[134] *Id.* at 110.
[135] Nehf, *Incomparability*, *supra* note 50, at 27 ("For individuals to protect their privacy interests, they must be able to identify the culprit who broke a law, breached a voluntarily adopted privacy policy, or allowed access to a database because of lax security procedures.").
[136] EU Directive, *supra* note 19, art. 8 (2) and (3).
[137] EU Directive, *supra* note 19, art. 8 (4).

Even with more mundane personally identifiable information, "the market approach provides *too little control* over personal data,"[138] partly because the United States' privacy policies are based on an opt-out regime, rather than an opt-in system.

This opt-out regime has a number of problems. One problem is that "[b]ecause personal information is valuable, easily collected, and often free; companies have strong incentives and virtually no disincentives to collect as much of it as they can."[139] Having an opt-out regime means that certain people, mainly those who are not savvy enough to read the privacy policies and opt-out of the collection, will be at a disadvantage.

Another problem is that "[i]f people are only vaguely aware of a data-sharing activity, they cannot evaluate the extent of any potential injury, and it is difficult for them to take protective measures or to stop the activity from recurring."[140] A self-help system assumes that individuals will be diligent in defending their privacy rights and that they have the ability to value their privacy rights meaningfully. For such an assumption to be warranted, the population must be sufficiently educated to be able to "make . . . informed choice[s] about whether and how to share information, and whether to take the time or spend the money to protect it."[141] Because individuals do not know what happens to their personally identifiable information after it is given out, or how it is combined with other aggregated data, "it is difficult to assess the risks associated with releasing information or failing to monitor its use after its release."[142]

B. Privacy Policies

Just about every business has a privacy policy. By buying an item, consumers tacitly agree to the seller's privacy policy. Sometimes, consumers actively agree to these policies, for example, by clicking "I agree" or clicking on a radio button stating that the consumer has read and understood the privacy policy and user terms and agreements. Privacy policies of businesses suffer several weaknesses: They lack uniformity, "they are cryptic or in small print no one reads, and [they are] subject to unilateral change."[143] Moreover, "an individual

---

[138] Kang & Buchner, *supra* note 12, at 244.
[139] McClurg, *supra* note 1, at 91.
[140] Nehf, *Incomparability*, *supra* note 50, at 20.
[141] *Id.* at 21.
[142] *Id.*
[143] Kang & Buchner, *supra* note 12, at 244.

cannot easily determine the actual consequences of disclosure."[144]

The consumer has little to no choice in the matter. If one wants to buy something from a business or read articles from a newspaper, one must agree to its privacy policy. There is no opportunity or ability to negotiate with the company. These privacy policies, in short, are contracts of adhesion, which provide only "a limited range of means for consumer redress."[145]

V. WHY NATIONAL LEGISLATION IS THE BEST OPTION

Federal legislation which would set a floor for privacy in the United States is the best way to resolve difficulties created by market failure, the confusion of competing state laws, and the inability of individuals to bring tort, contract and property claims. It would provide individuals and businesses with the best incentives to address and correct data privacy problems currently plaguing the United States.

The current piecemeal legislation, and the market-driven approaches that businesses have taken, have lead to gaps, overlaps, and inconsistencies among the different approaches. Since the Internet is not contained within one state or country, legislation has potential cross-border implications. As different states enact legislation, there is often no uniformity between key terms. For example, "key terms like 'personal information' are not consistently defined, creating discrepancies as to whether a company must disclose a security breach."[146] Federal statutes also contain their own definitions for key terms, further compounding this confusion. A comprehensive privacy statute, however, would bring all these different competing statutes into alignment, creating uniform definitions and legal standards and eliminating inconsistencies.

Without a comprehensive privacy statute in place, market forces have stepped into the void.[147] As discussed above, the market has proven itself to be insufficient in solving the problems of Internet privacy. A uniform federal privacy law would be a boon to companies as well as individuals, as there would be one standard to apply across the country, eliminating

---

[144] *Id.*

[145] Zaidi, *supra* note 55, at 172.

[146] Rode, *supra* note 114, at 1627 (citation omitted) (comparing security breach notification statutes in California, Georgia, Montana, and North Dakota and how each defines "personal information").

[147] Nehf, *Incomparability*, *supra* note 50, at 3 ("When no consensus emerges, policymakers do little or nothing and, for better or worse, market forces emerge as the de facto privacy regime.").

the conflicting standards that led companies to enact different security measures to avoid liability on a state-by-state basis. The current mélange of legislation and market forces "poses a threat to the viability of data collecting businesses [which] transforms the statutes from tools that foster useful market forces in terms of stimulating more responsible data into misfits that produce an environment of uncertainty, undermining companies' efforts to comply."[148] It would be in a business's own interest to support the passage of a comprehensive privacy regime, because such a regime would simplify the legislative minefield that business currently must traverse.

With increasing attention being given to privacy issues, states have stepped into the void left by the federal government and have begun enacting their own legislation.[149] As each state enacts its own legislation, with its own definitions and standards, businesses will face increasing complications in adhering to each individual state's legislation. This patchwork of state legislation will make "it difficult to establish a baseline privacy standard that consumers and businesses alike can follow."[150]

In addition, the general public is not only becoming more interested and concerned about how personally identifiable information is used, but also supports comprehensive reform. Sixty-nine percent of respondents to a recent survey believe that "there should be a law that [gives] people the right to know everything a Web site knew about them."[151] In the same survey, ninety-two percent of respondents supported a "hypothetical law that [would require] Web sites and advertising companies to delete all information about an individual upon request."[152]

Some critics of a national privacy law believe consumers should allow businesses to collect, aggregate and analyze their private data, because "(1) these data actually do some good, (2) the harm is actually not very great, and (3) no one spends money collecting these data to actually learn anything about you. They want to learn about people like you."[153] Furthermore, these critics warn that without the ability to collect and aggregate personal information, there will be higher marketing and distribution costs, as well as fewer new services and products because of the higher cost of introducing these to the public at

---

[148] Rode, *supra* note 114, at 1633.

[149] Towle, *supra* note 61.

[150] Zaidi, *supra* note 55, at 172.

[151] Stephanie Clifford, *Two-Thirds of Americans Object to Online Tracking*, N.Y. TIMES, Sept. 29, 2009, at B3.

[152] *Id.*

[153] LESSIG, *supra* note 104, at 151-152; DeMarco, *supra* note 96, at 1024.

large.[154] This "parade of horribles," however, is not likely to happen, as the example of Europe amply demonstrates:

> We see Europeans happy to use bonus cards and frequent traveler programs to receive discounts. They do not seem especially hesitant to disclose personal data in exchange for a free e-mail service or the chance to take part in a lottery. They are willing to sell their privacy for a couple of Euros, as are Americans for a couple of dollars.[155]

What the critics fail to recognize is that "data protection legislation is about the protection of individuals rather than the regulation of industry [and that it] is civil rights legislation rather than technical business legislation."[156] Privacy advocates do not seek to hinder companies from conducting business but to protect private personal data.[157]

Another criticism is that "adopting a European-style privacy policy may not fit with [American values such as] our constitutional traditions regarding free speech, our trust in the efficiencies of competitive markets, and our suspicion of government-imposed solutions to private-sector problems."[158] The difference between Europe and the United States with regards to privacy "can in fact be traced to the reality that the United States, unlike most Western European nations, does not have a literal constitutional basis for the treatment of privacy as a fundamental right."[159] Although free speech is an explicit right guaranteed by the United States Constitution,[160] the right to privacy is an implicit right guaranteed by the Constitution as interpreted by the United States Supreme Court.[161] The United

---

[154] *See* Svetlana Milina, Note, *Let the Market Do Its Job: Advocating an Integrated Laissez-Faire Approach to Online Profiling Regulation*, 21 CARDOZO ARTS & ENT. L.J. 257, 261-62 (2003).

[155] Kang & Buchner, *supra* note 12, at 261.

[156] DIANE ROWLAND & ELIZABETH MACDONALD, INFORMATION TECHNOLOGY LAW 307 (2005).

[157] Editorial, *Watching Your Every Move*, N.Y. TIMES, June 13, 2007, *available at* http://www.nytimes.com/2007/06/13/opinion/13wed3.html (arguing that "[p]rivacy is too important to leave up to the companies that benefit financially from collecting and retaining data.").

[158] Nehf, *Incomparability*, *supra* note 50, at 45.

[159] Moshell, *supra* note 3, at 364 n.53.

[160] U.S. CONST. amend. I.

[161] *See generally* Roe v. Wade, 410 U.S. 113 (1973) (finding the state cannot interfere in a woman's privacy when choosing whether to have an abortion); Griswold v. Connecticut, 381 U.S. 479 (1965) (deciding that the First, Third, Fourth, and Ninth Amendments together create an implied constitutional right to privacy in the marital relationship).

States Constitution grants citizens a right to privacy from government intrusion, but does not provide for a general right to privacy from private individuals. In contrast, many other countries have statutory[162] or constitutional[163] rights to personal privacy, which are enforceable against private individuals and entities as well as the government. In some countries, personal privacy is "viewed as a fundamental human right grounded in the dignity of the person."[164]

While the background of privacy law in the European Union is different from that of the United States, it is possible to create an omnibus privacy statute like the EU directive, which would be compatible with American cultural values. It is true, for example, that the EU Directive may have created freedom of speech issues within the European Union.[165] However, there are ways to protect this country's explicit freedom of speech values while also protecting peoples' private data. Congress could consider holding "[c]ommercial actors . . . to higher standards in the handling of citizens' personal data while allowing individual citizens not engaged in commercial or professional activities to use and disclose personal data on others."[166] Furthermore, if "there is a commercial component to an individual citizen's personal data processing, they would then be subject to the higher standard just as any other commercial actor is."[167] The protection of personal privacy does not seriously conflict with any provision of the Constitution.

Other critics have cautioned against rushing too hastily to pass a national privacy law.[168] Their "passive approach carries a

---

[162] *See, e.g.*, *ekomloven* [The Electronic Communications Act], July 4, 2003, No. 83, § 2-7 (Nor.), *translated in* Norway Post and Telecommunications Authority, *The Electronic Communications Act*, *available at* http://www.npt.no/ikbViewer/Content/ekom_eng.pdf?documentID=7922.

[163] *See, e.g.*, S. AFR. CONST., 1996, Ch. 2, § 14 ("Everyone has the right to privacy, which includes the right not to have: a. their person or home searched; b. their property searched; c. their possessions seized; or d. the privacy of their communications infringed.").

[164] Kang & Buchner, *supra* note 12, at 234.

[165] Harris, *supra* note 46, at 745 (using three cases before the European Court of Justice to show the conflict between United State's freedom of speech rights in conflict with EU Privacy Directive privacy law).

[166] *Id.* at 796.

[167] *Id.*

[168] *See* Nehf, *Shopping*, *supra* note 124, at 5-6 ("There is virtue in being patient when creating a national public policy to address a new and dynamic problem. The slow pace of privacy regulation in the United States, as compared to the rush to regulate in Europe, may be beneficial in the long run . . . . We are still in the relatively early stages of an emerging market for information privacy. Over time, market influences such as advertising, personal experience, privacy signals (such as privacy trust marks), and technological developments may make privacy terms more salient.").

price."[169] The longer the United States waits to enact privacy legislation, the longer it leaves individuals' privacy interests vulnerable to invasion while providing those individuals little to no legal recourse. In addition, when the sectoral manner of privacy legislation is allowed to persist, businesses and individuals will come to solidify their "attitudes about privacy . . . thus making it more difficult to change the status quo and initiate sweeping reforms at a later time."[170]

The United States need not fear that a comprehensive data protection scheme would quickly become outdated. The EU Directive, which was passed in 1995 and enacted by member states in 1998, debunks the claim that privacy legislation always becomes outdated and outmoded quickly. Indeed, the OECD Guidelines[171] were created in 1980 and have so far withstood the test of time. A general floor for privacy can weather and grow with the ongoing technological changes that increasingly impact personal privacy.[172] At the very least, a "comprehensive form of privacy protection will . . . act as a benchmark from which interested parties and relevant authorities may curb the misuses of online personal data.[173]

The United States should learn from the missteps taken by the European Union (such as problems with enforcement) and create a better system: "[L]egislation would probably not be effective in controlling information privacy unless it created a strong incentive for someone to enforce it."[174] There are other lessons to be learned from foreign privacy legislation of which the United States can and should be mindful while crafting its own.

---

[169] Nehf, *Incomparability*, *supra* note 50, at 56.

[170] *Id*. ("Arguments against policy change become stronger as vested interests become more entrenched.").

[171] ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT [OECD], GUIDELINES ON THE PROTECTION OF PRIVACY AND TRANSBORDER FLOW OF PERSONAL DATA (Sept. 23, 1980), *available at* http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html.

[172] In 1980, when the OECD Guidelines were created, few could have foreseen YouTube or Facebook. *See* Jaikumar Vijayan, *Blockbuster Sued Over Facebook Information Sharing*, COMPUTERWORLD, Apr. 18, 2008, http://computerworld.com/action/article.do?command=viewArticleBasic&taxonomyName=standards_and_legal_issues&articleId=9078938&taxonomyId=146 (describing how new problems arise as old and new technology combine as is seen in the current "class-action lawsuit against Blockbuster Inc. over the video rental company's participation in Facebook's Beacon program," which shares users "video tape rental and sales records with Facebook without seeking" the user's permission).

[173] Zaidi, *supra* note 55, at 197 ("The advantage of a comprehensive privacy regime is that it ultimately provides uniformity and certainty to such an objective.").

[174] McClurg, *supra* note 1, at 100.

VI. WHAT PROPOSED LEGISLATION SHOULD INCLUDE

The United States has its own historical reasons for lacking expressed, written constitutional or statutory provisions protecting privacy. Any comprehensive data privacy legislation in the United States, therefore, would need to be different from the European Union's privacy laws.

One of the things a comprehensive United States data privacy scheme should take from the EU Directive is the bar on exploiting sensitive data including "racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union memberships, and the processing of data concerning health or sex life."[175] This restriction would have a huge impact. The United States Census, for example, asks questions about racial and ethnic origin as well as religious or philosophical beliefs by inference. However, even with an omnibus privacy statute, legislation could make an exception to the rule for the census, or the census itself could ask each participant if he or she will consent to having his or her information gathered and processed, thus complying with a comprehensive data privacy scheme. Furthermore, the statute might place restrictions on what the government could do with the information after collecting it. For instance, it could provide that census information only be non-identifying information or that census information only be aggregated and reported after any personally identifying information has been stripped out.

The United States should also incorporate into the legislation the idea that "transfers of personal data to third countries"[176] must "ensure an adequate level of protection"[177] or else "be prohibited."[178] There is little point in enacting comprehensive data privacy legislation, which permits the outsourcing of data retention to a country that provides little to no privacy safeguards.[179]

---

[175] EU Directive, *supra* note 19, art. 8 (1).

[176] EU Directive, *supra* note 19, ¶ 56.

[177] *Id.*

[178] EU Directive, *supra* note 19, ¶ 57.

[179] *E.g.* Rachel Konrad, *Foreign Accountants Do U.S. Tax Returns*, USA TODAY, Feb. 4, 2004, *available at* http://www.usatoday.com/money/perfi/taxes/2004-02-23-overseas-outsourcing_x.htm. Sometimes workers in other countries attempt to use the information to get higher wages or additional money. For example, in October 2003, a medical transcription subcontractor in Pakistan sent an email with attached patient files to the University of California San Francisco Medical Center demanding payment. *See* Jay Fitzgerald, *Known Around the World, Private Records May Be at Risk*, BOSTON HERALD, Nov. 30, 2003, at 27; David Lazarus, *Extortion Threat to Patients' Records: Clients Not Informed of India Staff's Breach*, S.F. CHRON., Apr. 2, 2004, at A1; *see also* David Lazarus, *Looking Offshore: Outsourced UCSF Notes Highlight Privacy Risk: How One Offshore Worker Sent Tremor Through Medical System*, S.F. CHRON., Mar. 28, 2004, at A1.

The collection of personally identifiable information should be on an opt-in, rather than an opt-out system. Before the proliferation of cheap storage devices and before the rise of the Internet, transactional costs associated with an opt-in regime were prohibitive. However, "these costs may go to zero in the online world, and if that is the case then the economic argument against opt-in should be revisited."[180] Society has now reached this point, and any comprehensive data privacy legislation should require an opt-in rather than the current opt-out approach. The EU Directive takes such an approach by stating that "Member States shall provide that personal data may be processed only if . . . the data subject has unambiguously given his consent."[181]

In addition, individuals should be provided contact information so that they can access, modify, update, or remove their personally identifiable information from a company's records. The process of removing oneself from the company's records should be simple and fast. Companies should be banned from requiring individuals to fill out complex forms, mail them in, and then wait for weeks or months while the company makes changes.

Furthermore, individuals should be notified of "the purposes of the processing for which the data are intended."[182] The EU Directive sets forth this standard in Article 10.[183]

A comprehensive data scheme should take specific care not to tread on the strong First Amendment protections governing the freedom of speech. However, legislation should not allow "business interests that gather personal data and seek to protect that information under the First Amendment [to] pervert the idea of 'commercial speech' which was designed to protect consumers."[184]

Any legislation should also recognize the failures of the FTC's role and create a strong incentive for people to police how companies use and retain their personally identifiable information. Perhaps the legislation could create both a criminal and a private right of action.[185] Allowing a private citizen to bring an action would make businesses more likely to comply in

---

[180] Rotenberg, *supra* note 45, ¶ 114.

[181] EU Directive, *supra* note 19, Chap. I, § II, art. 7 (a).

[182] EU Directive, *supra* note 19, Chap. I, § IV, art. 10.

[183] *Id.*

[184] Marsha Cope Huie, et al., *The Right to Privacy in Personal Data: The EU Prods the U.S. and Controversy Continues*, 9 TULSA J. COMP. & INT'L L. 39, 426 (2002).

[185] The EU Directive "provide[s] for the right of every person to a judicial remedy for any breach of the rights guaranteed him." *See* EU Directive, *supra* note 19, Chap. III, art. 22.

the face of potential lawsuits. This incentive to comply would help turn the external costs of privacy security into internal costs for the company by making "it bad business for them not to care."[186]

Any legislation should not regulate privacy matters based on whether an issue arises online or offline. Information privacy arises in both the online world—through purchases, movie rentals, email sign-ups—and in the offline world of doctor's appointments, grocery purchases, and traffic tickets.

Any legislation should also mandate disclosure to the public and to the individuals whose security may be compromised in the event of a breach. It should not matter whether the company thinks there is a risk of identity theft; disclosure should be mandatory. A disclosure requirement may have the positive effect of publicly shaming a company "into improving its security." [187]

Finally, the law must not be so watered down as to be ineffective. Many states have enacted privacy legislation[188] and breach legislation.[189] Federal law should not offer lesser protections than those already in place around the country, thereby preempting more effective state laws.

VII. CONCLUSION

The time has come for Congress to enact comprehensive data privacy legislation for U.S. citizens, covering data acquisition, retention, and reuse. The current piecemeal, ad-hoc smattering of legislation and self-help remedies have done little to stem the tide of identity theft and lost records. This approach has failed to lessen the widespread aggregation and commoditization of personally identifiable information.[190]

A comprehensive data privacy scheme is needed because the market has proven insufficient at sorting out optimal privacy protections, which are of real benefit to anyone at the consumer level. In addition, the traditional common law remedies of tort,

---

[186] John Oates, *Bruce Schneier Talks Cyber Law*, THE REGISTER, Oct. 19, 2005, *available at* http://www.theregister.co.uk/2005/10/19/schneier_talks_law/.

[187] Bruce Schneier, *The Anti-ID-Theft Bill That Wasn't*, WIRED, Apr. 20, 2006, *available at* http://www.wired.com/politics/security/commentary/securitymatters/2006/04/70690.

[188] Electronic Privacy Information Center, Privacy Laws by State., http://epic.org/privacy/consumer/states.html (last visited Oct. 8, 2009).

[189] U.S. PIRG, SUMMARY OF STATE SECURITY FREEZE AND SECURITY BREACH NOTIFICATION LAWS, http://www.uspirg.org/financial-privacy-security/identity-theft-protection/summary-of-state-laws (last updated Jul. 18, 2006).

[190] Moshell, *supra* note 3, at 430-31. ("Experience shows that such changes will only occur when economic realities catch up to the United States and the cost of doing business in a globalized economy without comprehensive data protections outweighs the U.S. interest in self-regulation.").

contract, and property law are currently inadequate to protect privacy interests. The patchwork regulation and self-help methods available to individuals today do not do enough to limit improper uses of personally identifiable information.

Federal legislation is the best way to overcome the above problems. Congress can make policy decisions for the country, and it has the ability to create committees to study such problems and potential solutions. Indeed, "[c]onventional wisdom says that legislative and agency bodies are better venues for collecting information about social policy issues."[191]

While there are critics who maintain that any such protective legislation would be inefficient and have a negative impact on the economy, it is important to remember that "[e]fficiency does not always equate with justice."[192] The time has come to rein in what has been called the "Wild West era of online privacy"[193] and protect individuals' personally identifiable information.

[191] McClurg, *supra* note 1, at 99.
[192] *Id.* at 104.
[193] *Watching Your Every Move*, *supra* note 157.