LITTLE BROTHER'S BIG BOOK: THE CASE FOR A RIGHT OF AUDIT IN PRIVATE DATABASES

Preston N. Thomas[†]

I. INTRODUCTION

To even the most dedicated scholars, the concept of privacy has proven "exasperatingly vague and evanescent"[1] and "infected with pernicious ambiguities."[2] Because privacy is difficult to define, it does not fit neatly into existing legal frameworks.[3] Instead, privacy has produced years of "well-meaning but intractable debates."[4] English legal scholar and privacy advocate Raymond Wacks suggests that "[i]nstead of pursuing the false god of 'privacy', attention should be paid to identifying what *specific interests* of the individual we think the law ought to protect."[5]

Following this advice, many legal scholars grappling with the problem of protecting privacy have advocated a more operationalized view of privacy that breaks the abstract concept into concrete assertions more readily incorporated

---

[†] J.D. Candidate, May 2010, The Catholic University of America, Columbus School of Law. The author wishes to express his deep gratitude to the associates and editors of the *CommLaw Conspectus* for their hard work on this project.

[1] Daniel Solove, *"I've Got Nothing to Hide" and Other Misunderstandings of Privacy*, 44 SAN DIEGO L. REV. 745, 754 (2007) (quoting ARTHUR R. MILLER, THE ASSAULT ON PRIVACY: COMPUTERS, DATA BANKS, AND DOSSIERS 25 (1971)).

[2] *Id.* at 754 (quoting Hyman Gross, *The Concept of Privacy*, 42 N.Y.U. L. REV. 34, 35 (1967)).

[3] RAYMOND WACKS, PERSONAL INFORMATION: PRIVACY AND THE LAW 10–11 (1989). Wacks argues that a rights-based approach to privacy, as opposed to a holistic approach, will avoid forcing personal information problems into the "strait-jacket of 'privacy.'" *Id.* at 10.

[4] Marcy E. Peek, *Information Privacy and Corporate Power: Towards a Re-Imagination of Information Privacy Law*, 37 SETON HALL L. REV. 127, 128 (2006); Solove, *supra* note 1, at 754.

[5] WACKS, *supra* note 3, at 10. Writing primarily from the standpoint of English legal theory, Wacks cites American commentator R.F. Hixon who acknowledged that "a natural 'right' to privacy is simply inconceivable as a legal right . . . Privacy itself is beyond the scope of the law." *Id.*

into the legal system.[6] Like the Supreme Court's approach in *Miranda v. Arizona* that operationalized due process as a series of discrete rights,[7] privacy reform is best approached in small increments that avoid the paralysis historically associated with comprehensive reform. Abandoned efforts at privacy reform and dead comprehensive data protection statutes that sought to protect privacy—something they could not define—litter the halls of the United States Congress.[8] With privacy's amorphous nature and technology's ever-evolving nature,[9] the omnibus approach to privacy actually works against such reform materializing.[10]

To avoid this problem and to address the growing need for privacy reform, the solution should start small and be done deliberately piecemeal. Contrary to some advocates for comprehensive privacy reform,[11] piecemeal construction is not necessarily a bad thing. Many modern privacy and data protection rights were first established as a small nucleus that grew organically as political and practical realities changed.[12] To begin addressing the ever-increasing problem

---

[6] *See, e.g.*, Daniel J. Solove, *Conceptualizing Privacy*, 90 CAL. L. REV. 1087, 1091–92 (2002) (suggesting that our concept of privacy should be viewed through a pragmatic prism of how such a conception solves concrete social and legal problems).

[7] *Miranda v. Arizona*, 384 U.S. 436, 468–74 (1966) (operationalizing the broadly worded protections of the Fifth Amendment as a constellation of narrowly circumscribed rights that can be administered efficiently to improve the interrogation process for both the subject, by assuring him of his constitutionally guaranteed protections, and the police, by providing an easily implemented rule).

[8] *See, e.g.*, Online Privacy Protection Act of 2003, H.R. 69, 108th Cong. (2003) (requiring "the Federal Trade Commission to prescribe regulations to protect the privacy of personal information collected from and about individuals . . . not covered by the Children's Online Privacy Protection Act . . . to provide greater individual control over the collection and use of that information . . . ."); Data-Mining Reporting Act of 2004, H.R. 4290, 108th Cong. § 3 (2004) (requiring "[t]he head of each department or agency of the Federal Government that is engaged in any activity to use or develop data-mining technology . . . [to] submit a public report to Congress on all such activities . . . ."); Consumer Privacy Protection Act of 2005, H.R. 1263, 109th Cong. § 102 (2005) (requiring data collectors to establish privacy policies and to notify consumers when their personally identifiable information will be used for purposes unrelated to the transaction and to update consumers on material changes to the privacy policy).

[9] *See* Jonathan K. Sobel, et al., *The Evolution of Data Protection as a Privacy Concern, and the Contract Law Dynamics Underlying It, in* SECURING PRIVACY IN THE INTERNET AGE 55–56 (Anupam Chander et al. eds. 2008).

[10] *Id.* at 57.

[11] *See, e.g.*, Bruce Schneier, *Our Data, Ourselves*, WIRED, May 15, 2008, http://www.wired.com/politics/security/commentary/securitymatters/2008/05/securitymatters_0515 [hereinafter *Our Data, Ourselves*]; 153 CONG. REC. S1635-38 (daily ed. Feb. 6, 2007) (statements of Sens. Specter & Feingold) (introducing the Personal Data Privacy and Security Act of 2007).

[12] *See, e.g.*, Fair Credit Reporting Act, Pub. L. No. 91-508, 84 Stat. 1127 (1970) (codified as amended at 15 U.S.C. §§1681–1681x (2006)); Consumer Credit Reporting Reform Act of 1996 ("CCRRA"), Pub. L. No. 104-208, 119 Stat. 3009-426 (1996) (codified at 15 U.S.C. §§ 1681-1681x (2006)); Fair and Accurate Credit Transactions Act of 2003 ("FAC-

of diminishing data privacy, we need a narrow, simple principle that can act as an effective stopgap. Such a measure would provide some degree of near-term oversight and accountability of the watchers to the watched; it would also allow for legislative and judicial flexibility to deal with rapidly changing technology and services. This Comment proposes a private right of audit that would, at the very least, allow consumers "a look in the books" and a chance to inspect the information being collected about them. The proposed statute pragmatically balances the need for a broad new paradigm—information as a negative externality[13]—with the equally weighty need to fit solutions within the practical realities of politics and business.[14]

This Comment examines the contours of a specific legal interest within the suite of interests that comprise "privacy" in the context of commercial data storage. Part I briefly recaps how the collection of private information by commercial entities has developed from a trivial problem into a growing and discrete threat with real harms. This discussion encompasses commercial data's changing role and its new uses that affect private business, government actions and, ultimately, individual lives. Part II then details the broad base of legal and political support for the idea that data collection regimes, both governmental and private, should be accountable to the subjects of that data. While not exhaustive, the discussion highlights some of the important touchstones of modern data privacy, including past, current, and proposed legislation, busi-

---

TA"), Pub. L. No. 108-59, 117 Stat. 1952 (2003) (codified at 15 U.S.C. § 1681 and 20 U.S.C. § 9701-9708) (2006). The 1996 CCRRA added, among other changes, the concept of "adverse actions" against the consumer and further refinements of the disputed information procedures. § 2411, 110 Stat. 3009-426, 443–45 (codified at 15 U.S.C. § 1681m). The 2003 FACTA contained many notable changes in addition to providing for free annual credit reports, including requiring the industry to develop "red flag" rules to spot identity theft and allowing "affiliate sharing" subject to consumer disclosure and choice. §114, 117 Stat. 1952 at 1960-61 (codified at 15 U.S.C. § 1681m); §214, 117 Stat. 1952 at 1980-83 (codified at 15 U.S.C. § 1681s).

[13] *See* Bruce Schneier, *The Tech Lab: Bruce Schneier*, BBC ONLINE, Feb. 26, 2009, http://news.bbc.co.uk/1/hi/technology/7897892.stm [hereinafter *The Tech Lab*] (asserting that data is "a natural by-product of every computer-mediated interaction. It stays around forever, unless it's disposed of. It is valuable when reused, but it must be done carefully. Otherwise, its after-effects are toxic.").

[14] The business community—and, correspondingly, congresspersons on behalf of their industry constituency—has traditionally opposed privacy reform efforts. *See, e.g.*, Joel Michael Schwartz, *A 'Case of Identity': A Gaping Hole in the Chain of Evidence of Cyber-Crime*, 9 B.U. J. SCI. & TECH. L. 92, 115–16 (2003) (comparing the privacy and criminal issues of public terminals with commercial mail receiving agencies and noting the opposition to new regulations for commercial mail receiving agencies by businesses "were characteristic of their interests."); Gregory Schaffer, *Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting Up of U.S. Privacy Standards*, 25 YALE J. INT'L L. 1, 44 (2000) (discussing President Bill Clinton's administration's defense of businesses in negotiating over the European Union approaches to issues in data privacy). *But see infra* Part III for a discussion of the growing support for change.

ness best practices, and international principles. Part III analyzes the advantages and disadvantages of the diverse practical and legal approaches often employed when attempting to address harms associated with private data aggregation. Finally, Part IV presents and weighs the various components of a right of audit, suggesting those that are truly central to establishing an effective right and explaining why some components could ultimately prove counterproductive.

II. WATCHING THE WATCHERS

A. Junk Mail and Credit Card Offers?

As Daniel Solove argues in *"I've Got Nothing to Hide" and Other Misunderstandings of Privacy*, there is little interest in protecting oneself from apparently innocuous data gathering,[15] which may simply result in more advertising. An everyday example of data gathering occurs at supermarkets, which use information they obtain from customer loyalty cards to send consumers targeted coupons and advertisements.[16] Although many consumers using these loyalty cards realize that the stores they patronize track their purchasing habits, this data mining does not bother most consumers enough to give up the use of these loyalty cards.[17] As one Kroger customer said, "If it was anything else, it might be different . . . . But it's groceries. So, what the heck? Who cares who knows what I eat?"[18] This reflexive indifference, a typical reaction to private sector data gathering in most industries, extends from the common man all the way to Supreme Court justices. Justice Antonin Scalia said that information to be considered private "doesn't include what groceries I buy," unless the infor-

---

[15] Solove, *supra* note 1, at 756 (recognizing that the majority of information in data banks is not "sensitive" information, which he defines as information which would inhibit people's activities if the information were known).

[16] Dan Sewell, *The Price of Loyalty*, EXPRESS (Wash., D.C.), Jan. 9, 2009, at 31. The Kroger Company, an American supermarket chain, also has an ownership stake in the data-mining firm DunnhumbyUSA, which also has contracts with Coca-Cola Co., Home Depot Corp., Procter & Gamble Co., Macy's Inc., and Kraft Foods Inc. *Id.*

[17] *Id.*

[18] *Id.* One consumer's observations on data mining indicates that the practice is so pervasive that some consumers simply give up on avoiding it, saying:

> We all have more demographic labels attached to us in various databases than we'll ever know, and thinking about it would make me insane, so I just do what I can to limit my exposure to them and let the rest go. The amount of work required to be free of it all would probably result in me living in a cave as a hermit.

Martin H. Bosworth, *Alternatives to Loyalty Cards: Retail Chains Largely Mum About Their Policies*, CONSUMER AFFAIRS, Aug. 3, 2005, http://www.consumeraffairs.com/news04/2005/loyalty_cards2.html.

mation is "shameful."[19] This concept is the essence of the "nothing to hide" argument: the perception that an interest in privacy necessarily arises from an immoral or unethical desire to hide something.[20] Thus, advocates for privacy and personal information reform in the private sector have had a hard time gaining traction because the visible harms are not weighty and the weighty harms are not visible.

B. It's Not Just Groceries Anymore: Broader and Deeper Collection, Wider Dissemination and Use

The threat of private data aggregation is rapidly becoming less trivial for several reasons.[21] The collection of personal information has become broader and deeper in keeping with a series of related developments: the wholesale adoption of information technology in business, the digitization of records traditionally kept on paper, and the deliberate combining and mining of these data stores.[22] That is, more areas of our public lives are being recorded, and they are being recorded in greater depth and detail than in the past.[23]

The scope of the privacy problem has expanded in every direction. More entities now keep more records on more people than in the past. Acxiom, the world's largest data aggregator, holds information on ninety-six percent of American households.[24] Richard Behar explains that "[o]nce upon a time in

---

[19] Posting of Daniel Solove, *Justice Scalia's Dossier: Interesting Issues about Privacy and Ethics*, to Concurring Opinions, http://www.concurringopinions.com/archives/2009/04/justice_scalias_2.html (Apr. 29, 2009, 10:43 EST). When presented with a fifteen page dossier of his personal information compiled by a class at the Fordham University School of Law, Scalia characterized the compilation as "an example of perfectly legal, abominably poor judgment." He did not make clear whether this pronouncement extended to corporate entities engaged in for-profit aggregation or was limited to law students working on a class project. *Id.*

[20] Solove, *supra* note 1, at 764; *see also* Richard A. Posner, *Privacy, Secrecy, and Reputation*, 28 BUFF. L. REV. 1, 11 (1979) (describing one sense of privacy as "the concealment of discreditable facts about oneself" as "closely related to reputation" since "it is a method . . . of enhancing reputation.").

[21] *See* Bruce Schneier, Op-Ed., *Your Vanishing Privacy: Welcome to the World of Wholesale Surveillance, Where Many Entities Track People's Electronic Footprints*, MINN. STAR TRIB., Mar. 5, 2006, at AA1 [hereinafter *Your Vanishing Privacy*] (describing the correlation between the increase in computer usage for transactions and the increase in the information from those transactions being stored, analyzed, and repurposed).

[22] *The Tech Lab*, *supra* note 13 (imagining a future "where everything about you is saved. A future where your actions are recorded, your movements are tracked, and your conversations are no longer ephemeral. A future brought to you not by some 1984-like dystopia, but by the natural tendencies of computers to produce data.").

[23] *See Your Vanishing Privacy*, *supra* note 21.

[24] Marcy E. Peek, *Beyond Contract: Utilizing Restitution to Reach Shadow Offenders and Safeguard Information Privacy*, *in* SECURING PRIVACY IN THE INTERNET AGE 137 (Anupam Chander et al. eds., 2008).

America a savvy store clerk knew that you had, say, three kids, an old Ford, a pool, and a passion for golf and yellow sweaters. Today Acxiom is that store clerk . . . . [but] [i]t manages 20 billion customer records . . . ."[25] ChoicePoint, another data broker, "owns an astounding 19 billion records, about 65 times as many pieces of information as there are people in the United States."[26] With such vast amounts of information in its hands, ChoicePoint likely has more information on most individuals than the federal government does.[27]

Instead of the usual public record information such as name, address, phone number, and date of birth, the data kept is as varied as the activities individuals engage in.[28] For instance, Acxiom groups individuals by "lifestyle clusters" that reflect the constellation of activities and traits Acxiom knows about the individual.[29] This sort of dossier-building can be as detailed as the information sources that feed it.[30] While in the past these dossiers have largely been comprised of public records, today companies combine additional sources of information, such as customer loyalty cards and even Web site cookies, to create profiles of individuals that are much more useful for business purposes—and are more concerning to the individuals behind these profiles.[31] One corporation, Verified Identity Pass Inc., has gone even further: as part of the Registered Traveler program, Verified Identity Pass collected biometric information—fingerprints and even retinal scans—from clients in exchange for expedited security processing at airports.[32]

---

[25] Richard Behar, *Never Heard of Acxiom?*, FORTUNE, Feb. 23, 2004, at 142. *See also* Acxiom, Acxiom Corporation Company Overview, http://www.acxiom.com/overview (last visited Sept. 9, 2009) (describing the company as the "developer of some of the largest and most sophisticated business intelligence and marketing databases in the world . . . .").

[26] Shane Harris, *Private Eye*, GOVERNMENT EXECUTIVE, Mar. 16, 2004, http://www.govexec.com/features/0304/0304s1.htm. ChoicePoint is now wholly owned by the parent company of LexisNexis, Reed Elsevier. LexisNexis ChoicePoint, Overview, http:// www.choicepoint.com/about/overview.html (last visited Oct. 8, 2009).

[27] Harris, *supra* note 26.

[28] Joseph Apfelroth, *Regulating Commercial Data Brokers in the Wake of Recent Identity Theft Schemes*, 2 BUS. L. BRIEF 33, 33 (2005).

[29] Behar, *supra* note 25, at 144 (explaining that Acxiom's lifestyle clusters "rang[e] from 'Rolling Stones' and 'Single City Struggles' to 'Timeless Elders.'").

[30] *See Identity Theft: Recent Developments Involving the Security of Sensitive Consumer Information Before the S. Comm. on Banking, Hous., & Urban Affairs*, 109th Cong. 2 (2005) (statement of Deborah Platt Majoras, Chairman, Fed. Trade Comm'n).

[31] *See* Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083, 1092–93 (2001).

[32] Samantha Bomkamp, *Unclear What Happens to Personal Info with Clear*, June 26, 2009, USA TODAY.COM, http://www.usatoday.com/travel/flights/2009-06-29-clear-personal-data_N.htm. Verified Pass Inc. has since folded. A notice on its Clear program Web site pledges that any personal identification sold would "not be used for any purpose other than a Registered Traveler program operated by a Transportation Security Administration authorized service provider." Clear, Clear Lanes Are No Longer Available, http://flyclear.com/ (last visited Aug. 27, 2009).

Data brokers, however, merely represent the most visible face of private-sector data collection.[33] Even companies not explicitly in the business of collecting customer data can and do compile significant records through contact with consumers.[34] Retail behemoth Wal-Mart serves 100 million customers a week, nearly a third of the U.S. population.[35] From these transactions it has compiled nearly sixty-five terabytes of data on its customers.[36] Additionally, "affiliate data sharing" programs disseminate customer records to companies with whom the customer may not have an established relationship.[37] Affiliate data sharing is the industry term for one business sharing its customer records with another business; this could be a bank sharing records with another bank,[38] or even, under a proposed Internal Revenue Service rule, a tax preparer selling tax return information directly to a data broker.[39]

---

[33] *See, e.g.*, *Your Vanishing Privacy*, *supra* note 21; Harris, *supra* note 26.

[34] *See, e.g.*, Sewell, *supra* note 16 (listing Coca-Cola Co., Home Depot Corp., Procter & Gamble Co., Macy's Inc., and Kraft Foods Inc. as other clients of data-broker DunnhumbyUSA); *see also* Constance L. Hays, *What They Know About You*, N.Y. TIMES, Nov. 14, 2004, at BU1.

[35] Hays, *supra* note 34 (noting that with such a volume of sales, "Wal-Mart has access to information about a broad slice of America - from individual Social Security and driver's license numbers to geographic proclivities for Mallomars, or lipsticks, or jugs of anti-freeze."); *see* CIA, The World Factbook: United States, https://www.cia.gov/library/publications/the-world-factbook/geos/us.html (follow "People :: United States" hyperlink) (last visited Sept. 10, 2009) (estimating the U.S. population in July 2009 to be 307,212,123 people) [hereinafter The World Factbook].

[36] To illustrate how much data sixty-five terabytes actually provides, consider that more than 650 text-only (ASCII) files (such as information that would be kept in a purchasing records database) can fit into one megabyte. With the U.S. population at approximately 300 million people, sixty-five terabytes of data means that Wal-Mart's servers have enough data to compile the equivalent of a 150-page dossier on the purchasing habits of every man, woman, and child in the United States. That is a lot of groceries. *See* Setec Investigations, Inc., *How Many Pages per Gigabyte and Megabyte?*, http://www.setecinvestigations.com/resources/techhints/Pages_per_Gigabyte.pdf (giving approximate numbers of documents which can be carried in different memory units); The World Factbook, *supra* note 35.

[37] Chris Hoofnagle, Op-Ed., *Is Your Life an Open Book? And Who's Reading It?*, AKRON BEACON J. (Akron, Ohio), Sept. 8, 2003, at B3. ChoicePoint and Acxiom's use of the terms "individual" and "household" in lieu of "customer" is telling. While this comment uses these terms interchangeably, the most accurate term to describe this asymmetric relationship is arguably "subject."

[38] *See id.*

[39] Prop. Treas. Reg. § 7216, 70 Fed. Reg. 72954 (Dec. 8, 2005) (examining "proposed regulations to update the rules regarding the disclosure and use of tax return information by tax return preparers. The proposed regulations announce new and additional rules for taxpayers to consent electronically to the disclosure or use of their tax return information by tax return preparers."); *see also* Electronic Privacy Information Center, *Comments to IRS on Tax Return Info Sharing*, Mar. 8, 2006, http://epic.org/privacy/tax/irscom3806.html (discussing how the proposed rules could lead to ineffective consent and unscrupulous disclosure of tax records).

The significant role of the Internet in American society means that the information garnered from a user's online activities provides a significantly more comprehensive, nuanced, and "deeper" view of the individual than might be assembled from twentieth-century methods like loyalty cards and public records.[40] In 2006, America Online (now AOL) intentionally released "anonymized" search results of 657,000 subscribers.[41] However, to AOL's chagrin, the allegedly anonymized data released quickly proved how even anonymous Web search records are actually highly informative, highly personal, and in many cases, highly identifiable.[42] Similarly, in 2008, Viacom Corporation subpoenaed the entire viewing history, including usernames and IP addresses, of the online video-sharing service YouTube as part of its copyright infringement suit against Google.[43] DoubleClick, an online advertising company, now owned by Google,[44] has the ability to examine and "merge" cookies from disparate Web sites to generate a significantly more comprehensive picture of a user's online activities than would be available to any one operator.[45] In the world of Internet service providers ("ISPs"), companies like United States-based NebuAd, now defunct,[46] and United Kingdom-based Phorm[47] recently piloted

---

[40] *See The Tech Lab*, *supra* note 13 (explaining that computer-mediated transactions allow information to be saved more easily, accessed more widely, and combined more readily).

[41] Declan McCullagh, *AOL's Disturbing Glimpse into Users' Lives*, CNET NEWS, Aug. 7, 2006, http://news.cnet.com/2100-1030_3-6103098.html.

[42] *Id.* (providing numerous illustrations of how search queries are a widely eclectic mix of the mundane and the deeply personal). For example, one AOL user searched for "calories in bananas" before moving on to searching for "can you adopt after a suicide attempt" and "divorce laws in ohio" [sic]. *Id. See also* Michael Barbaro & Tom Zeller Jr., *A Face is Exposed for AOL Searcher No. 4417749*, N.Y. TIMES, Aug. 9, 2006, at A1 (illustrating how anonymized Web search information can be traced back to particular individuals because of the richer and more comprehensive sources of data than previous forms).

[43] Miguel Helft, *Google Told to Turn Over User Data of YouTube*, N.Y. TIMES, July 4, 2008, at C1.

[44] Louise Story & Miguel Helft, *Google Buys DoubleClick for $3.1 Billion*, N.Y. TIMES, Apr. 14, 2007, at C1.

[45] *See* George R. Milne, *Privacy and Ethical Issues in Database/Interactive Marketing and Public Policy: A Research Framework and Overview of the Special Issue*, 19 JOURNAL OF PUBLIC POL'Y & MARKETING 1, 4 (2000), *available at* http://www.atypon-link.com/AMA/doi/pdf/10.1509/jppm.19.1.1.16934.

[46] *See* Posting of Scott Austin, *Turning Out the Lights: NebuAd,* to WSJ BLOGS: VENTURE CAPITAL DISPATCH, http://blogs.wsj.com/venturecapital/2009/05/19/turning-out-the-lights-nebuad/ (May 19, 2009, 7:52 EST).

[47] Phorm, Inc., http://www.phorm.com/index.php (last visited Aug. 27, 2009); Phorm, Inc. Advertising, http://advertising.phorm.com (last visited Aug. 27, 2009) ("By partnering directly with ISPs, [Phorm's platform service] can draw from the greatest supply of browsing information and avoid the limitations of purely site-based data."); *see also* Darren Waters, *Home Office 'colluded with Phorm'*, BBC NEWS, Apr. 28, 2009, http://news.bbc.co.uk/2/hi/technology/8021661.stm (stating that "Phorm serves up adverts related to a user's web browsing history that it monitors by taking a copy of the places they

business models based on partnering with ISPs to create profiles of Internet users and serve them with targeted ads.[48] The privacy concerns over this invasive technique and the resulting data were illustrated during a 2008 hearing of the House Subcommittee on Telecommunications and the Internet where NebuAd CEO Bob Dykes affirmed that individual consumer profiles would be kept anonymous and secure and would be purged if a user chose to opt-out of having his data collected.[49] Congressman Cliff Stearns challenged Dykes' assertions that users' profiles do not contain information the user views on "sensitive subjects," asking, "how do we know that you avoid that? I mean, we just take your word for it?"[50] While the Congressional scrutiny helped result in the shuttering of NebuAd[51] and the suspension of the British ISP BT's use of Phorm's services,[52] Congressman Stearn's question remains unanswered.

In addition to the broadening and deepening of personal information collection, data collection systems are also becoming more centralized. Data brokers like Acxiom and LexisNexis, which acquired ChoicePoint in September 2008,[53] have created comprehensive, individual profiles that are more than the sum of their parts.[54]

C. "The Fourth Amendment Two-Step": Private Collection, Government Use

The real revelation, however, is not in how private entities are collecting personal information; it is in how that information is being used. Because the

---

go and search terms they look for.").

[48] Austin, *supra* note 46 (describing NebuAd's ability, through its partnership with ISPs, to monitor users' "activities across multiple Web sites without their express permission"); Jacqui Cheng, *UK ISP Drops Phorm Behavioral Ad Tech—for Now*, ARS TECHNICA, July 6, 2009, http://arstechnica.com/telecom/news/2009/07/uk-isp-ditches-plans-for-behavioral-ad-techfor-now.ars.

[49] *See What Your Broadband Provider Knows about Your Web Use: Deep Packet Inspection and Communications Laws and Policies*: *Hearing before the H. Subcomm. on Telecommunications and the Internet*, 109th Cong. 1–8 (2008) (statement of Bob Dykes, CEO, NebuAd, Inc.), *available at* http://archives.energycommerce.house.gov/cmte_mtgs/110-ti-hrg.071708.Dykes-testimony.pdf.

[50] John Timmer, *Markey to NebuAd: "When did you stop beating the consumer?"*, ARS TECHNICA, July 17, 2008, http://arstechnica.com/business/news/2008/07/markey-to-nebuad-when-did-you-stop-beating-the-consumer.ars.

[51] *See* Austin, *supra* note 46.

[52] Hannah Benjamin, *BT Delays Use of Phorm Service*, WSJ.COM, July 6, 2009, http://online.wsj.com/article/SB124689052552600797.html.

[53] LexisNexis ChoicePoint, Overview, http:// www.choicepoint.com/about/overview.html (last visited Oct. 8, 2009).

[54] *See, e.g.*, ChoicePoint, Frequently Asked Questions About Your ChoicePoint Full File Disclosure, http://www.choicepoint.com/documents/ffd_faqs.pdf (last visited Oct. 8, 2009) ("ChoicePoint consumer files contain a compilation of various information about individuals that we maintain in our consumer reporting databases.").

government has had, and continues to have, an enormous role in affecting the rights and lives of its citizens, government surveillance has long been viewed as "far more ominous" than when the private sector engages in similar activities.[55] While Richard A. Posner, prior to serving as a judge on the United States Court of Appeals for the Seventh Circuit, dismissed appeals for privacy in the private-sector context as presumptively manipulative and injurious to the orderly operation of society,[56] the reality of modern private data collection, both its scope and its potential use by government entities, should give him pause.[57] With the rise of the Internet and massive private data collection, the United States government has increasingly turned to privately held information as a way to bolster its knowledge about its citizens.[58] This partnership has blurred the line between privately held data and government data, resulting in a quandary for Posner and the worst of both worlds for consumers: unregulated private collection combined with highly consequential government use.[59] The FBI is one of many government agencies that routinely purchases information from ChoicePoint to supplement its investigations; in fact, one FBI agent admitted that "[t]he success of an investigation is often directly proportional to the information [from ChoicePoint] we can gather on suspects."[60] The information

---

[55] Richard A. Posner, *The Uncertain Protection of Privacy by the Supreme Court*, 1979 SUP. CT. REV. 173, 176 (positing that the rationale for viewing government surveillance as more ominous is because "[t]he government is not subject to the discipline of the marketplace which will punish a private firm or individual who demands information beyond the point where the value of the information equals the price of obtaining it."); *see also The Government Sector: The Greatest Menace to Privacy By Far*, PRIVACILLA.ORG, Sept. 2000, http://www.privacilla.org/releases/Threats_to_Privacy.html (cataloguing the extraordinary reach of government surveillance programs past and present, including Carnivore, Echelon, Know Your Customer, National Individual Health IDs, CALEA, and the Clipper Chip).

[56] Posner, *supra* note 55, at 175–76.

[57] *Id.* at 176. Posner recognized this distinction noting, "Where, however, the information is not sought by members of the public, acting as it were in self-protection, but by the government, the claim of privacy as secrecy is stronger." *Id.*

[58] *See* Arshad Mohammed & Sara Kehaulani Goo, *Government Increasingly Turning to Data Mining*, WASH. POST, June 15, 2006, at D3 (citing the profiling of teenagers for potential military recruiting and travelers for border searches); *see also* Posting of Ryan Singel, *Flying Without ID? Know What's in Your Files*, to Threat Level, http://www.wired.com/threatlevel/2008/07/flying-without/ (July 18, 2008, 16:43 EST) (citing a TSA program that uses LexisNexis information to quiz air travelers on their personal information if they are unable to produce their identification).

[59] To be fair, Posner has since recognized this quandary. Richard A. Posner, *Privacy, Surveillance, & Law*, 75 U. CHI. L. REV. 245, 257 (2008) ("The government's ready access to the vast databases that private and public entities compile for purposes unrelated to national security has enabled it to circumvent much of the protection of privacy that civil libertarians look to warrant requirements to secure.").

[60] Harris, *supra* note 26, at 33–34; *see also* Associated Press, *Obama Keeps Some Bush Secrets*, MSNBC.COM, Apr. 19, 2009, http://www.msnbc.msn.com/id/30292790 ("[T]here is no public list of all the databases the FBI sucks into this computer warehouse; no information on how individuals can correct errors about them in this FBI database; and no public

held by private data aggregators is driving government action in areas such as the Federal Aviation Administration's No-Fly List, background checks, and increased border scrutiny.[61]

Julian Sanchez, paraphrasing Judge Posner, has characterized this common situation as the "Fourth Amendment Two-Step": when privately held information that the government could not constitutionally gather on its own is instead acquired from non-governmental third-parties.[62] The first step of this end run is found in the logic of *California Bankers Ass'n v. Shultz*, which concerned a provision of the Bank Secrecy Act of 1970 requiring that banks keep records of their transactions and make them available to the government upon request.[63] The Supreme Court held that such a requirement does not violate the Fourth Amendment because the government "neither searches nor seizes records in which the depositor has a Fourth Amendment right."[64] The second step is found in *United States v. Miller*, which held that banks could be required to maintain records of their customers' transactions and that individuals lose their "expectation of privacy" in such information when they turn it over to a bank or another third party.[65] This principle, that transactional data is presumptively unprotected, continued three years later in *Smith v. Maryland*, in which the Supreme Court extended the *Miller* rationale to phone numbers, finding that individuals "know that they must convey numerical information to the phone company," and therefore they cannot "harbor any general expectation that the numbers they dial will remain secret."[66]

Less than ten years after *Miller*, *California v. Greenwood* presaged security researcher and author Bruce Schneier's conception that "[d]ata is the pollution

---

access to assessments the bureau did of the warehouse's impact on Americans' privacy.").

[61] *See, e.g.*, *Our Data, Ourselves*, *supra* note 11; Singel, *supra* note 58; Behar, *supra* note 25 (explaining that the TSA's Computer Assisted Passenger Pre-Screening System ("CAPPS II") program, since discontinued due to privacy concerns, was largely driven by data from Acxiom).

[62] *See* Julian Sanchez, *The Fourth Amendment Two-Step*, TECHDIRT, Jan. 27, 2009, http://www.techdirt.com/articles/20071127/173344.shtml.

[63] California Bankers Ass'n. v. Shultz, 416 U.S. 21, 54 (1974) (finding that the Bank Secrecy Act of 1970 does not violate the Fourth Amendment by requiring banks to maintain records which are then available to the government via subpoena).

[64] *Id.*

[65] *See* United States v. Miller 425 U.S. 435, 442–43 (1976), *partially superseded by statute*, Right to Financial Privacy Act of 1978, Pub. L. No. 95-630, tit. XI, 92 Stat. 3697 (codified as amended at 12 U.S.C. §§ 3401-22 (2006)), *as recognized in* SEC v. Jerry T. O'Brien, Inc., 467 U.S. 735, 745 (1984). The Supreme Court held that the government did not violate a bank customer's Fourth Amendment rights when the government subpoenaed the bank for the customer's bank records because "the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose . . . ."). *Id.* at 443.

[66] Smith v. Maryland, 442 U.S. 735, 743 (1979).

of the information age."[67] In the context of physical garbage, the Supreme Court ruled that it is "common knowledge that . . . [trash] left on or at the side of a public street [is] readily accessible to animals, children, scavengers, snoops, and other members of the public."[68] The result of the "Fourth Amendment Two-Step" and the later cases is a legal conduit of personal information from the citizen, through private data banks, and into government hands.[69] Posner, himself no friend of privacy,[70] nonetheless has observed that the *Miller* line of cases is "unrealistic . . . about the meaning of . . . 'privacy' itself."[71]

The House Committee on Energy and Commerce's 2007 investigation of the National Security Agency ("NSA") and the telecommunications industry highlights this conduit.[72] The investigation concerned the voluntary, warrantless disclosure of millions of customers' phone records by phone companies in violation of section 222 of the Communications Act of 1934.[73] The law and the private sector have created an efficient industry that "allow[s] law enforcement to buy access to intricate dossiers on American citizens it couldn't otherwise collect."[74]

---

67 *The Tech Lab*, *supra* note 13; California v. Greenwood, 486 U.S. 35 (1988).

68 *Greenwood*, 486 U.S. at 40. *But see id.* at 45 (Brennan, J., dissenting) ("Scrutiny of another's trash is contrary to commonly accepted notions of civilized behavior.").

69 *See* Solove, *supra* note 1, at 765 (stating that "the lack of Fourth Amendment protection of third party records results in the government's ability to access an extensive amount of personal information with minimal limitation or oversight."); *see also* Solove, *supra* note 31, at 1085–86, 1090–93.

70 Judge Posner has written extensively on the value and disvalue of privacy, particularly from an economic standpoint. His analyses are well known for their repeated conclusions that privacy is economically (and therefore legally) inefficient. *See e.g.*, Richard A. Posner, *Privacy, Secrecy, and Reputation*, 28 BUFF. L. REV. 1, 11–12 (1979) (likening privacy to a seller trying to cover up defects); Richard A. Posner, *The Economics of Privacy*, 71 AM. ECON. REV. 405, 406 (1981) (likening privacy to a prospective employee or spouse attempting to conceal character deficiencies); Posner, *supra* note 55, at 174 (likening privacy to a police applicant concealing serious mental illness). For a defense of the value of privacy, *see* Bruce Schneier, Commentary, *The Eternal Value of Privacy*, WIRED.COM, May 18, 2006, http://www.wired.com/news/columns/1,70886-0.html.

71 RICHARD A. POSNER, NOT A SUICIDE PACT: THE CONSTITUTION IN A TIME OF NATIONAL EMERGENCY 140 (2006).

72 Letter from John Dingell, Ed Markey, and Bart Stupak, U.S. Representatives, to Randall L. Stephenson, Chairman & CEO, AT&T (Oct. 2, 2007), *available at* http://energycommerce.house.gov/images/stories/Documents/PDF/Letters/110-ltr.100207.TI.ATTStephenson.pdf. The U.S. is not the only governmental example. The U.K. Home Office consulted with Phorm on the legality of Phorm's operation, and apparently allowed Phorm to assist in drafting the Home Office Opinion. Waters, *supra* note 47.

73 47 U.S.C. § 222 (2006) (prohibiting disclosure of customer proprietary information except as required by law or with customer's approval); Dingell et al., letter, *supra* note 72.

74 Nicole Duarte, *Commercial Data Use by Law Enforcement Raises Questions about Accuracy, Oversight*, CARNEGIE-KNIGHT INITIATIVE ON THE FUTURE OF JOURNALISM EDUCATION, Aug. 16, 2006, http://newsinitiative.org/story/2006/08/16/commercial_data_use_by_law.

These examples illustrate that the potential harm of data aggregation by private parties has changed with the amount and type of data collected; it is no longer confined to the seemingly trivial invasion of increased advertising. Instead, private data aggregation now encompasses the non-trivial threats of invasive use, misuse, and loss of the data, as well as the possibility that it can be acquired and used by the government in ways that avoid constitutional and statutory protections. In 1977, even before the modern era of computing and networking, the U.S. Privacy Protection Study Commission concluded that "[t]he real danger is the gradual erosion of individual liberties through the automation, integration, and interconnection of many small, separate record-keeping systems, each of which alone may seem innocuous, even benevolent, and wholly justifiable."[75]

To explain the nature of the privacy threat from this ubiquitous "Little Brother" data collection, Solove proposes a corollary to the typical characterization of privacy intrusions in terms of George Orwell's dystopia.[76] Instead of casting private-sector data collection as the Orwellian-style surveillance state usually identified with government and law enforcement, Solove characterizes private-sector data collection as analogous to Franz Kafka's *The Trial*, in which a "bureaucracy with inscrutable purposes uses people's information to make important decisions about them yet denies the people the ability to participate in how their information is used."[77] This model recognizes that information technology consolidates power, and information asymmetries invariably affect the relationships between people and the institutions that make important decisions in their lives.[78] The basic fact, which Kafka recognized in 1956 and Schneier articulated in 2008, that "who controls our data controls our lives"[79] must be translated into meaningful statutory action.

---

[75] U.S. PRIVACY PROTECTION STUDY COMM'N, PERSONAL PRIVACY IN AN INFORMATION SOCIETY 533 (1977) (emphasis omitted).

[76] *See* Solove, *supra* note 1, at 756–57.

[77] *Id.* (citing FRANZ KAFKA, THE TRIAL 50–58 (Willa & Edwin Muir, trans., Random House 1956) (1937)).

[78] *See* SERGE GUTWIRTH, PRIVACY AND THE INFORMATION AGE 85 (Raf Casnet trans., Rowman & Littlefield (2002)); Solove, *supra* note 1, at 757.

> [T]he problems caused by surveillance . . . affect the power relationships between people and the institutions . . . . They not only frustrate the individual by creating a sense of helplessness and powerlessness, but they also affect social structure by altering the kind of relationships people have with the institutions that make important decisions about their lives.

Id.

[79] *Our Data Ourselves*, *supra* note 11; *accord* Paul M. Schwartz, *Privacy and Participation: Personal Information and Public Sector Regulation in the United States*, 80 IOWA L. REV. 553, 560 (1995) (arguing that the use of data banks by the government and private organizations "creates a potential for suppressing a capacity for free choice: the more that is known about an individual, the easier it is to force his obedience.").

D. The Need for Accountability

Schneier observes that nearly all day-to-day activities leave a permanent digital record:

> This data shadow doesn't just sit there: It's constantly touched. It's examined and judged . . . . Whoever controls our data can decide whether we can get a bank loan, on an airplane or into a country. Or what sort of discount we get from a merchant, or even how we're treated by customer support. A potential employer can, illegally in the U.S., examine our medical data and decide whether or not to offer us a job.[80]

Thus, there is a current and accelerating "personal information alienation," and that alienated information is being put to use in increasingly expansive ways that affect the individual to whom they pertain.[81] Schneier and others have called for a comprehensive data privacy law,[82] but enacting such a law may be more difficult than it appears. Despite growing recognition of the potential harm of data collection, comprehensive data protection laws have been introduced but have not been enacted.[83] This is in large part due to the slippery nature of the concept of "privacy," in addition to the American conception of data as belonging to the collector rather than the subject.[84]

As evidenced by the staggering depth and breadth of largely unregulated data collection, the current legal regime is inadequate for the task of addressing the complex relationship between an individual, his or her information, and the company that holds it. In an article examining government use of commercial databanks, Nicole Duarte found that "many of America's most important privacy protections do not apply to commercial data brokers."[85] Professor Marcy

---

80 *Our Data Ourselves*, *supra* note 11.

81 PEEK, *supra* note 24, at 138. Other commentators have argued that

> [o]ver the past few decades, there have been dramatic expansions in the quality, the breadth, and the intensity of programs that use new generations of technology for gathering, storing, sharing, and using information . . . . [I]f we add up the frequently overlapping profiles encompassing medical records, academic and professional performance, credit ratings, consumer behavior, insurance records, driving records, law enforcement data, welfare agency information, child support enforcement programs, Internet communications, and other information systems, it is safe to say that much of the significant activity of our lives is now subject to systematic observation and analysis.

JOHN GILLIOM, OVERSEER OF THE POOR: SURVEILLANCE, RESISTANCE, AND THE LIMITS OF PRIVACY 2 (2001).

82 *Our Data Ourselves*, *supra* note 11.

83 *See* Online Privacy Protection Act of 2003, H.R. 69, 108th Cong. (2003); Data-Mining Reporting Act of 2004, H.R. 4290, 108th Cong. § 3 (2004); Consumer Privacy Protection Act of 2005, H.R. 1263, 109th Cong. § 102 (2005).

84 *See Your Vanishing Privacy*, *supra* note 21 (noting that after "the dot-com bust, the customer database was often the only salable asset a company had."); Aaron Titus, *When Did My Personal Information Become Your Property?*, SECURITY CATALYST, http://www.securitycatalyst.com/when-did-my-personal-information-become-your-property (last visited Sept. 20, 2009).

85 Duarte, *supra* note 74.

E. Peek terms these third party information dealers "[s]hadow offenders"[86] because they have no business relationship with the individuals they monitor; in fact, they are generally unknown to society as a whole.[87] Because data brokers are not in privity of contract with users, users cannot sue them on a contract theory, and thus "third-party entities have little incentive to protect, or even ensure the accuracy of, personal data."[88] What is needed is a minimal, baseline level of accountability of the watcher to the watched. Thankfully, there is substantial and growing legal and political support for exactly this sort of privacy legislation.

III. LEGAL AND POLITICAL WILL FOR CHANGE

Numerous federal and state laws, agency decisions, and public policies have begun to slowly incorporate the idea of disclosure, audit, and responsibility to the individual.[89] Although it is beyond the scope of this Comment to catalog them all, an overview of a representative sample will illustrate the growing consensus that responsible and socially acceptable data collection must incorporate certain elements, in particular, the right of audit.

A. Legislative Efforts

In the context of some legislative efforts, "required disclosure" means a data collector's obligation to "clearly and accurately" convey to the consumer what information the collector has on him or her.[90] The most prominent example of required disclosure is found in the Fair Credit Reporting Act ("FCRA").[91] Prompted by Congress' recognition that private credit bureaus had "grave responsibilities" to act with "fairness, impartiality, and a respect for the con-

---

86 PEEK, *supra* note 24, at 139.

87 *See* Behar, *supra* note 25 (providing that Acxiom's customers "include nine of the country's top ten credit-card issuers, as well as nearly all the major retail banks, insurers, and automakers."). At Acxiom, people—or at least their digital doppelgangers—are a product, not a customer.

88 PEEK, *supra* note 24, at 139; *see also* Julian Sanchez, *Secrecy Plus Immunity Eliminates Accountability,* TECHDIRT, Nov. 7, 2007, http://www.techdirt.com/articles/20071106/155324.shtml (suggesting that the general paradigm of not requiring disclosure and failing to have a framework for corrective action invariably removes all incentives, save for "public-spiritedness," for companies to reject government demands for the personal data those companies have collected).

89 *See infra* Part III.A–D.

90 Fair Credit Reporting Act, 15 U.S.C. § 1681g (a) (2006).

91 Fair Credit Reporting Act, 15 U.S.C. § 1681–1681x. *See generally* Electronic Privacy Information Center, The Fair Credit Reporting Act (FCRA) and the Privacy of Your Credit Report, Sept. 22, 2007, http://www.epic.org/privacy/fcra/ (providing a readable history of the Act).

sumer's right to privacy," the FCRA was the federal government's first statutory attempt to regulate the use of personal information by private businesses.[92] The basic principles found in the FCRA would be used to lay the ground work for subsequent data privacy legislation;[93] foremost among these principles was a right of audit and correction.[94] In 2003, Congress strengthened these principles by passing the Fair and Accurate Credit Transactions Act ("FACTA"), which allows individuals to request a free annual credit report from each of the credit bureaus,[95] as well as the ability to opt-out of pre-approved credit offers[96] that can be both a nuisance and an identity theft risk. As Sobel et al. have observed, "[t]his simplistic approach . . . [of] notice . . . consent and access . . . has become the mantra to protect individual privacy rights nearly three decades after its passage."[97] The rationale behind passage of the FCRA was that consumers were being adversely affected by financial institutions having inaccurate credit scores on them and that consumers were having a difficult time keeping accurate track of their credit score.[98] Despite the broad applicability of its principles,[99] the FCRA was limited to credit reporting agencies.[100] While the FCRA does not extend to data aggregators, the Federal Trade Commission ("FTC") has concluded that were data aggregators to expand their dossiers to include credit information, they would likely fall within the FCRA.[101]

Several other notable statutes followed the principles contained in the FCRA. The Financial Modernization Act of 1999, commonly known as the Gramm-Leach-Bliley Act ("GLBA"), is a successor in spirit to the FCRA.[102] Narrow in its applicability like the FCRA, the GLBA is limited to financial institutions' disclosure of financial information, and relies on notice and opt-out as its main tools for regulating the relationship between the subject and the data collector.[103] Beyond the realm of financial information, the Health Insur-

92 15 U.S.C. § 1681 (a) (2006); *accord* Sobel et al., *supra* note 9, at 57–58.

93 *See* Fair Credit Reporting Act, Pub. L. No. 91-508, § 602, 84 Stat. 1127, 1128 (1970) (codified at 15 U.S.C. § 1681(b)); *see* SOBEL ET AL., *supra* note 9, at 58 (providing that the Act "requires that credit reporting agencies follow 'reasonable procedures' to protect the confidentiality, accuracy, relevancy, and proper utilization of credit information.")

94 Sobel et al., *supra* note 9, at 58.

95 15 U.S.C. § 1681j (a)(1)(A) (2006).

96 *See* 15 U.S.C. § 1681j (a)(1)(A) (2006); *see* Daniel J. Solove, *The New Vulnerability: Data Security and Personal Information*, *in* SECURING PRIVACY IN THE INTERNET AGE 111, 116 (Anupam Chander et al., eds., 2006).

97 Sobel et al., *supra* note 9, at 58.

98 *See* 15 U.S.C. § 1681 (2006).

99 *See* 15A Am. Jur. 2D *Collection and Credit Agencies* § 34 (2009).

100 *See* Sobel et al., *supra* note 9, at 57–58.

101 Letter from William Haynes, Attorney, FTC, to Sylvia Sum, Esq. (Sept. 15, 1999), *available at* http://www.ftc.gov/os/statutes/fcra/sum.shtm (providing an advisory opinion that data aggregators likely fall under the FCRA).

102 *See* Sobel et al., *supra* note 9, at 58.

103 *Id.*

ance Portability and Accountability Act of 1996 ("HIPAA")[104] applies the principles of disclosure, opt-out, access, and correction to an individual's health information and medical records.[105] Both the GLBA and the HIPAA, like the FCRA, are notable for their limitation of otherwise broadly applicable principles to specific industries.[106] The Children's Online Privacy Protection Act ("COPPA") changed this pattern by focusing on a particular class of individuals rather than an industry.[107] While mainly targeted at ISPs, COPPA provides rights of access, modification, and deletion across all businesses that may have contact with children.[108]

Because of the amorphous nature of "privacy," legislative efforts have focused on "specific areas of perceived abuse and vulnerability,"[109] rather than on comprehensive reform. This has resulted in a statutory framework that provides only sectoral vindication of broadly applicable interests.[110]

B. Agency Principles

In contrast to the industry-specific approach taken by legislators, many federal agencies have recognized the need for broadly applicable principles that hold true regardless of the actor or the industry.

The 1973 "Code of Fair Information Practices" ("CFIP")[111] is a particularly strong example of the "bundle of sticks" approach to defining responsible data collection. The Code is a result of an extensive study by the Advisory Commit-

---

[104] Pub. L. No. 104-191, 110 Stat. 1936 (1996) (codified in scattered sections of 26, 29, and 42 U.S.C.).

[105] 45 C.F.R. § 164.524 (2008) (describing rights of disclosure and access); 45 C.F.R. § 164.526 (2008) (describing a right of correction); *see also* SOBEL ET AL., *supra* note 9, at 58–59.

[106] *See* Sobel et al., *supra* note 9, at 57–58; *see also* discussion *infra* Part III.B, of the CFIPP and the FIPP, which proposes principles similar to those in the FCRA as being best practices, broadly applicable to data collection across all industries.

[107] *See* 15 U.S.C. § 6501 (2006); SOBEL ET AL., *supra* note 9, at 59.

[108] Sobel et al., *supra* note 9, at 59.

[109] *Id.* at 57.

[110] *See id.* (arguing that the piecemeal approach has left significant holes in privacy protection); Suzanne M. Thompson, *The Digital Explosion Comes With a Cost: The Loss of Privacy*, 4 J. TECH. L. & POL'Y 3, 31 (1999) (explaining that "[t]here are no universal fair information guidelines or practices that can be applied to ensure the protection and privacy of personal information. Under the U.S. scheme, no single standard cuts across boundaries of law or industry practice." (citation omitted)). *See also infra* Parts III.B and Part IV, for a discussion of the components of data privacy which are broadly recognized but inconsistently protected by existing statutory and common law frameworks.

[111] SEC'Y'S ADVIS'Y COMM. ON AUTOMATED PERSONAL DATA SYSTEMS, RECORDS, COMPUTERS, AND THE RIGHTS OF CITIZENS, U.S. DEP'T OF HEALTH, EDUCATION, AND WELFARE, CODE OF FAIR INFO. PRACTICES xx–xxi (1973) [hereinafter FAIR INFO. PRACTICES]; *see also* SOLOVE, *supra* note 96, at 124.

tee on Automated Data Systems, which was established by the Department of Health, Education, and Welfare (now the Department of Health and Human Services).[112] The CFIP, as the name implies, lays out the practices required to ensure that a data collection system is fair to its subjects. Two of the five conclusions of the CFIP stand for a right of audit. The second and third principles of the Code are, respectively, "[t]here must be a way for a person to find out what information about the person is in a record and how it is used," and "[t]here must be a way for a person to correct or amend a record of identifiable information about the person."[113] However, because the Department of Health and Human Services' Privacy Rule extends only to "covered entities," the CFIP principles have not been applied as generally as they might otherwise be.[114] Thus, the CFIP does not have a great deal of weight, despite its early and important formulation.[115]

By contrast, the FTC, which has adopted a very similar suite of principles, has a large and growing role in the regulation of data storage and privacy.[116] The FTC's "Fair Information Practice Principles" ("FIPP") are an attempt to crystallize the "core principles of privacy protection"[117] and include an emphatic acknowledgement of the role of the subject, including requirements of

---

[112] FAIR INFO. PRACTICES, *supra* note 111, at xix.

[113] Solove, *supra* note 96, at 124.

[114] U.S. Dep't of Health and Human Servs., Health Information Privacy: Covered Entities, http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/index.html (last visited Aug. 30, 2009).

> [Only] [i]ndividuals, organizations, and agencies that met the definition of a covered entity under HIPAA must comply with the Privacy Rule's requirements to protect the privacy of health information and must provide individuals with certain rights with respect to their health information. If an entity is not a covered entity, it does not have to comply with the Privacy Rule.

Id.

[115] Solove, *supra* note 96, at 124 (calling the CFIP "the most coherent and well-established set of duties that have been articulated for the use of personal data.").

[116] 15 U.S.C. § 45(a)(1); *see* Sobel et al., *supra* note 9, at 64 (providing that in regulating data privacy issues, "[t]he FTC relies on its authority to regulate 'unfair or deceptive acts or practices in or affecting commerce' under Section 5 of the Federal Trade Commission Act"); *see also* Jim Walden et al., *Data Breaches Mean More Than Bad Publicity*, N.Y.L.J., May 15, 2008, http://www.law.com/jsp/legaltechnology/pubArticleLT.jsp?id=1202421396867 (noting that in 2006, the FTC created the Division of Privacy and Identity Protection to investigate data breaches. By March 2008, the FTC had investigated many businesses and brought twenty cases against businesses that allegedly had not taken reasonable security measures to protect "sensitive consumer information"). *See generally Legislative Hearing on H.R. 2221, the Data Accountability and Protection Act, and H.R. 1319, the Informed P2P User Act*, H. Subcomm. on Commerce, Trade, and Consumer Protection, 111th Cong. (2009) (statement of the FTC), *available at* http://www.ftc.gov/os/2009/05/P064504peertopeertestimony.pdf (describing the Commission's position and efforts on protecting consumers' data security).

[117] *See* FED. TRADE COMM'N, FAIR INFORMATION PRACTICE PRINCIPLES (1998), *available at* http://ftc.gov/reports/privacy3/fairinfo.shtm [hereinafter FIPP].

access, redress, and participation.[118]

Additionally, in 1988, several defense-related agencies refused to turn over employee addresses, concerned that such disclosure would be a "clearly unwarranted invasion" of privacy.[119] In *Department of Defense v. F.L.R.A.*, the Supreme Court ruled in favor of the agencies,[120] recognizing that "[a]n individual's interest in controlling the dissemination of information regarding personal matters does not dissolve simply because that information may be available to the public in some form."[121] Justice Scalia, quoted earlier regarding an individual's privacy interest, or lack thereof, in their groceries,[122] joined the majority opinion.[123]

C. Multinational Acknowledgement

Foreign governments and multinational organizations have also arrived at the same conclusions, with remarkable consistency. While a full exploration of the recurring constellation of personal data rights in international law is beyond the scope of this Comment, the importance of foreign and multinational formulations to the development of privacy principles cannot be overstated. Several resources provide valuable insight into the legal and social understanding of privacy abroad.[124]

D. Private Sector Practices

The private sector itself has also acknowledged that consumer access is good for business. LexisNexis, a leading data storage company, provides in their privacy policy a restatement of their "Data Privacy Principles," which touches on many of the same elements as the FTC's FIPP and the former De-

---

118 *Id.*

119 U.S. Dep't of Defense v. F.L.R.A., 510 U.S. 487, 489 (1994). The case began after two labor unions sought, for the purpose of collective bargaining, employee names and home addresses from the U.S. Dept. of Defense and the U.S. Dept. of the Navy. *Id.* at 490.

120 *Id.* at 504.

121 *Id.* at 500.

122 Solove, *supra* note 19.

123 510 U.S. at 489.

124 *See, e.g.*, RAYMOND WACKS, PERSONAL INFORMATION: PRIVACY AND THE LAW 42–49, 204–230 (1989) (observing approaches to privacy laws in Britain). *See generally* INTERNATIONAL PRIVACY, PUBLICITY AND PERSONALITY LAWS (Michael Henry, ed. 2001) (comparing legal and social conceptions of privacy across many countries, in light of the laws and rights recognized); *see also* SERGE GUTWIRTH, PRIVACY AND THE INFORMATION AGE 87 (Raf Casert trans., Rowan & Littlefield Pub. 2002) (finding that the right of access and the right of correction are among the core principles common to the various successive European directives).

partment of Health, Education, and Welfare's CFIP.[125] LexisNexis' "Access and Correction" principle allows individuals to review personally identifiable information it maintains about them, although LexisNexis does not appear to accept corrections directly from the subject.[126] Similarly, Acxiom has "Global Privacy Principles" and "U.S. Product Privacy Principles," both of which include a right of notice, access, and correction.[127]

E. Reform Initiatives

Finally, there has been significant legislative effort toward data privacy reform. Several promising, comprehensive bills have been proposed in the last several Congresses, but each has died along the way.[128] The most recent version of a comprehensive personal data reform bill is S. 1490, the Personal Data Privacy and Security Act of 2009 ("the Act").[129] The Act prominently contains a right of review that applies to data brokers as well as civil penalties for violation.[130] Despite the valuable components in the Act, it also makes some subtle but important missteps in implementation that will be discussed in Part IV. Nonetheless, the Act's reoccurring presence on the Senate docket[131] indicates a will for change and support for holding data collectors accountable to those whose data they collect. In addition, the House of Representatives declared January 28, 2009 as "National Data Privacy Day" in an effort to "encourage[] individuals across the Nation to be aware of data privacy concerns and to take steps to protect their personal information online."[132]

While introducing the 2007 version of the Personal Data Privacy and Security Act, Senator Patrick Leahy declared that the right of consumers to review the sensitive personal information that data brokers have on them is "a simple

---

[125] *Compare* LexisNexis, *Data Privacy Principles*, http://www.lexisnexis.com/privacy/data-privacy-principles.aspx (last visited Sept. 2, 2009), *with* FAIR INFO. PRACTICES, *supra* note 111, *and* FIPP, *supra* note 117.

[126] LexisNexis, *supra* note 125.

[127] *See* Acxiom, Global Privacy Principles, http://www.acxiom.com/about_us/privacy/Pages/Privacy.aspx (last visited Sept. 2, 2009) (describing general policy principles); Acxiom, Highlights for U.S. Products Privacy Policy, http://www.acxiom.com/about_us/privacy/consumer_information/highlights_for_US_product_privacy_policy/Pages/HighlightsforUSProductsPrivacyPolicy.aspx (last visited Sept. 2, 2009) (offering the public the ability to access and correct information in Acxiom's directory for a processing fee of five dollars).

[128] *See, e.g.*, Data Security Act of 2007, H.R. 1685, 110th Cong. (2007); Data Accountability and Trust Act, H.R. 958, 110th Cong. (2007).

[129] *See* Personal Data Privacy and Security Act of 2009, S. 1490, 111th Cong. (2009).

[130] S. 1490, §§ 201–202.

[131] *See* Personal Data Privacy and Security Act of 2007, S. 495, 110th Cong. (2007); Personal Data Privacy and Security Act of 2005, S. 1789, 109th Cong. (2005).

[132] H.R. Res. 31, 111th Cong. (2009).

matter of fairness" for which there is "clear precedent" in U.S. law.[133] International policy, good business practice, and growing consumer demand also support the idea that the collectors of personal data have a fundamental obligation to the individual.[134] While there are several options for addressing consumer privacy concerns, a limited right of audit is a more proactive and more feasible method of ensuring accountable and responsible data collection.

IV. POSSIBLE ALTERNATIVE LEGAL APPROACHES TO A SOLUTION

In addressing problems associated with personal data collection, courts have generally relied on traditional elements of law, such as tort and contract.[135] Unfortunately, the practices of data collection and the harms associated with its misuse do not map well onto the established legal frameworks.[136] Part IV examines some of the legal and practical approaches to personal data accountability.

A. Effective Disclosure and Opt-in

"Closed Loop Confirmed Opt In" ("opt-in") is an industry best practice—part law and part procedure—which ensures consumers awareness about the collection and use of personal information about them, and requires their active consent for such collection and use.[137] In this sense, opt-in is firmly rooted in

---

[133] 153 CONG. REC. S1628 (daily ed. Feb. 6, 2007) (statement of Sen. Leahy).

[134] *See, e.g.*, Remarks of Christine A. Varney, Commissioner, Fed. Trade Comm'n, *Consumer Privacy in the Information Age: A View from the United States* (Oct. 9, 1996), *available at* http://www.ftc.gov/speeches/varney/priv&ame.shtm (noting that consumer demand for privacy grew out of increased data-gathering capabilities in the same way that increased data-gathering grew out of the burgeoning global information economy); LexisNexis, Data Privacy Principles, *supra* note 125; Acxiom Privacy Principles, *supra* note 127 (recognizing privacy protection as good business policy); APEC, APEC Privacy Framework, http://www.apec.org/apec/news___media/fact_sheets/apec_privacy_framework.html (last visited Sept. 2, 2009); Official Journal of the European Communities of 23 November 1995 No L. 281, Council Directive 95/46, art. 12, *available at* http://www.cdt.org/privacy/eudirective/EU_Directive.html (recognizing the data subject's right of access to their personal data as a fundamental policy).

[135] *See* Walden et al., *supra* note 116 (discussing the case law and implications of information torts); *see also* Peek, *supra* note 24, at 138–47 (discussing the uses and shortcomings of contract and quasi-contract-based approaches to data privacy violations).

[136] *See, e.g.*, Ann Bartow, *A Feeling of Unease about Privacy Law*, 154 U. PA. L. REV. PENNUMBRA 52, 52 (2006), *available at* http://works.bepress.com/cgi/viewcontent.cgi?article=1000&context=ann_bartow (critiquing Solove's privacy analysis for "fram[ing] privacy harms in dry, analytical terms that fail to sufficiently identify and animate the compelling ways that privacy violations can negatively impact the lives of living, breathing human beings beyond simply provoking feelings of unease.").

[137] Chris Thompson, *Confirmed Opt In: A Rose by Any Name*, SPAMHAUS, Aug. 11,

the contract law principle of informed consent, and it is a critical component of a framework for improving the collection of personal data.[138] Opt-in requirements solve "the most egregious inequality of the current opt-out system: the disparity in knowledge between the average user and the company collecting information."[139] Properly deployed, this approach ensures that customers and subjects are aware of the collection and how the information will be used. This is an important first step that is easily implemented and is therefore widely used (albeit at varying levels of earnestness) by companies who wish to collect information.[140] However, opt-in only goes so far in addressing the problem because it only affects data collection at the threshold point, when it is first collected from the customer.[141] Responsible data collection does not ensure that future uses of the data are equally responsible.[142] Thus, while opt-in is an important part of responsible data collection, it is insufficient by itself.

B. Breach Notification

Nearly every state in the country has enacted breach notification legislation.[143] As defined in California Civil Code section 1798.82, the statute that started the trend toward nationwide breach notification laws,[144] a breach means

---

2008, http://www.spamhaus.org/news.lasso?article=635 ("Closed Loop Confirmed Opt In is the full technical term for the best opt-in subscription practice around.").

[138] *See* Sobel et al., *supra* note 9, at 57–58 (characterizing the constellation of rights, including opt-in, provided by various data protection statutes as contractual and quasi-contractual in nature).

[139] Andrew Hotaling, Comment, *Protecting Personally Identifiable Information on the Internet: Notice and Consent in the Age of Behavioral Targeting*, 16 COMMLAW CONSPECTUS 529, 557–58 (2008) (noting that opt-in forms a foundation to further data rights in that "[w]ithout knowledge of the companies' identities, users have no means of correcting the inequality and reasserting some measure of control over their privacy on the Web.").

[140] *See* Anupam Chander, *Introduction*, *in* SECURING PRIVACY IN THE INTERNET AGE 6 (Anupam Chander et al., eds. 2008) ("Consent, a seemingly simple idea, is much less clear when faced in terms of opt in and opt out, pre-ticked tick boxes, half-buried links to privacy policies, and incomprehensible legal language.") (quoting Lilian Edwards, *The Problem with Privacy: A Modest Proposal*, 18 INT'L REV. L. COMP. & TECH. 309, 323 (2004)).

[141] *See* Edwards, *supra* note 140, at 320.

[142] *See, e.g.*, Solove, *supra* note 1, at 757–59 (explaining Solove's taxonomy of privacy intrusions that differentiates the information collection from later states of information processing and information dissemination).

[143] Nat'l Conference of State Legislatures, State Security Breach Notification Laws, http://www.ncsl.org/programs/lis/cip/priv/breachlaws.htm (last visited Sept. 2, 2009) (providing that forty-five states, the District of Columbia, Puerto Rico, and the Virgin Islands have laws requiring data holders to notify subjects of breaches that involve personal information).

[144] Cal. Civ. Code § 1798.82 (West Supp. 2009); *see also* Alan M. Mansfield, *Is Your Client Prepared To Comply With the Data Security Breach Notification Laws?*, ASS'N BUS. TRIAL LAW. REP., Spring 2007, at 15, *available at* http://www.abtl.org/report/sd/abtl-report-spring-2007.pdf.

"unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business."[145] Thus, breach notification is the simple principle that the subject of the data has a right to know and the holder of the data has a duty to disclose what has become of his or her data if the security of that data has been compromised.[146] These laws have helped protect those affected by data breaches and have pressured companies to strengthen their data protection policies.[147] However, breach notification can only do so much. By their nature, these laws are remedial rather than proactive; they do not provide the subject of the data any notification until it has been lost.[148] In addition, breach notification laws typically do not cover the legal and intentional uses of a subject's information about which the subject may nonetheless wish to be informed.[149]

Unlike opt-in and breach notification laws that provide victims with specific actions at law for the exposure of their information, much data-breach litigation is pursued using laws not specific to the collection of personal data.[150] Courts and case law primarily approach the problem through "causes of action grounded in tort and contract."[151]

---

[145] § 1798.82(e). "Personal information" is defined as

> an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted: Social security number, Driver's license number or California Identification Card number, account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account, medical information, or health insurance information.

Id.

[146] *See* Bruce Schneier & Marcus Ranum, *State Data Breach Notification Laws: Have they Helped?*, INFORMATION SECURITY MAGAZINE, Jan. 2009, http://searchsecurity.techtarget.com/magazineFeature/0,296894,sid14_gci1344729,00.html (explaining one rationale behind breach notification laws as "common politeness that when you lose something of someone else's, you tell him.").

[147] Pam Greenberg, *Right to Know*, STATE LEGISLATURES, Dec. 2008, at 26–27, *available at* http://ecom.ncsl.org/magazine/articles/2008/08sldec08_right.pdf; *see also* Chander, *supra* note 140, at 4 (observing that after a massive data breach in 2005, data broker ChoicePoint initially planned to only disclose the breach to California residents as was required under California law). Complaints from affected individuals across the country caused ChoicePoint to notify impacted consumers even in states without breach notification laws. *Id.*

[148] *See* Schneier & Ranum, *supra* note 146 (characterizing breach notification laws as being more effective at "butt-covering and paperwork than improving systems security.").

[149] *See, e.g.*, Cal. Civ. Code § 1798.82 (2009) (focusing on a "breach" as the primary threat, resulting from an overly narrow conception of personal data privacy).

[150] Walden et al., *supra* note 116.

[151] *Id.* (listing "negligence, breaches of fiduciary duty, breaches of real and implied contracts, invasion of privacy and emotional distress . . . [and] state law, such as consumer protection acts, unfair trade practices acts and state data breach notification laws.").

C. Tort Action

Tort law could provide a framework for victims of privacy abuses to be made whole and, at the same time, punish and deter bad actors. In 1890, Samuel Warren and Louis Brandeis introduced the common law privacy rights by framing the privacy protections in the language of tort law,[152] a conception that was eventually included in the Restatement (Second) of Torts.[153] Data breach cases provide an example of how the facts of a typical privacy violation fair on the negligence rubric of duty, breach, causation, and harm.[154]

1. Duty

The duty to protect and maintain the confidentiality of information can be can be inferred from any one or more of the patchwork of privacy laws such as the Graham-Leach-Bliley Act ("GLBA").[155] Despite its comprehensiveness, however, the GLBA may not be well suited to supplying the duty element to support a tort claim. In *Guin v. Brazos Higher Education Service Corp.*, a plaintiff filed suit against a student loan provider for negligence in exposing his personal information.[156] Guin claimed that under the GLBA, Brazos Higher Education Corp. ("Brazos") had a duty to protect customers' nonpublic personal information.[157] Brazos conceded that under the GLBA it had a duty of care for the protection of such information.[158] The district court ultimately held, however, that Brazos' actions were not inconsistent with the duty of care created under the GLBA and granted Brazos' motion for summary judgment.[159] The failure of this approach illustrates how the idiosyncratic obligations of the data privacy patchwork can undermine attempts to rely on them in the pursuit of tort law remedies.

---

[152] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 211–20 (1890).

[153] RESTATEMENT (SECOND) OF TORTS § 652d (1977). *But see* Solove, *supra* note 1, at 755 (rejecting Brandeis & Warren's conception of privacy as "the right to be left alone" as far too broad to perform meaningful legal work).

[154] *See* RESTATEMENT (SECOND) OF TORTS § 281 (1965).

[155] *See* Michael L. Rustad & Thomas H. Koenig, *Extending Learned Hand's Negligence Formula to Information Security Breaches*, 3 I/S: J.L. & POL'Y FOR INFO. SOC'Y 237, 242 (2007) (suggesting that those who are injured by data breaches protected by the GLBA could use a negligence *per se* argument to hold the data holder liable).

[156] Guin v. Brazos Higher Educ. Services Corp., 2006 U.S. Dist. LEXIS 4846, *1 (D. Minn. Feb. 7, 2006).

[157] *Id.* at *8.

[158] *Id.* at *8–9.

[159] *Id.* at *10.

2. Breach

The breach component, at least in the case of data breach cases, is more straightforward. According to Judge Learned Hand's formula from *United States v. Carroll Towing Co.*, a breach occurs when the respondent fails to take precaution commensurate with the risks.[160] Thus, merely showing a failure to reasonably secure the data (under the Learned Hand formula) or a failure to comply with applicable statutes (such as the GLBA) will, when combined with exposure, be sufficient to show breach.

3. Harm

Damage is the most difficult element for a plaintiff to prove in a data breach case. As the court explained in *Randolph v. ING Life Ins. & Annuity Co.*, when surveying a series of data breach cases, a plaintiff's "allegation of increased risk of identity theft . . . without more, is insufficient to demonstrate a cognizable injury."[161] These cases illustrate the typical pattern of data breach cases and explain why tort law has been largely unsuccessful in addressing data privacy concerns. The law is hesitant to provide a remedy for the de minimus harm of increased exposure to identity theft, and unwilling to consider mere "feelings of unease"[162] in that analysis.[163] As law professor Ann Bartow has explained, "[the] lack of blood and death, or at least of broken bones and buckets of money, distances privacy harms from other categories of tort law."[164] Especially with regard to the element of harm, this distance is often too great to utilize tort law as a practical remedy for data privacy violations.

D. Contract Actions

As discussed in the context of opt-in, the theory of contract law is also applicable to data privacy protection. In fact, Sobel et al., argue that the data pri-

---

[160] United States v. Carroll Towing Co., 159 F.2d 169, 173 (2nd Cir. 1947) (noted in Rustad & Koenig, *supra* note 155, at 242).

[161] Randolph v. ING Life Ins. & Annuity Co., 486 F. Supp. 2d 1, 14–15 (D.D.C. 2007) (citing Giordano v. Wachovia Sec., LLC, No. 06-476, 2006 WL 2177036, at *4 (D. N.J. July 31, 2006); Stollenwerk v. Tri-West Healthcare Alliance, No. 03-0185PHXSRB, 2005 WL 2465906, at *4 (D. Ariz. Sept. 6, 2005); Guin v. Brazos Higher Ed. Services Corp., No. 05-668, 2006 WL 288483, at *5 (D. Minn. Feb. 7, 2006); Bell v. Acxiom Corp., No. 06-485, at *3 (E.D. Ark. Oct. 3, 2006); Key v. DSW, Inc., 454 F. Supp. 2d 684, 690 (S.D. Ohio 2006)).

[162] *See* Bartow, *supra* note 136, at 52.

[163] *See* cases cited *supra* note 161.

[164] *Id. But see* Solove, *supra* note 1, at 768 (providing examples of cases where victims have been murdered by assailants who were able to locate the victims by obtaining their personal information from public records).

vacy debate to date has been "conducted over an unacknowledged tectonic plate of contract principles."[165] Like "privacy torts," however, contract actions have only had limited success. While corporate privacy policies or terms of service may appear to provide courts with a firmer basis for finding a breach of duty, courts have concluded that "broad statements of company policy do not generally give rise to contract claims."[166] Additionally, the peripheral nature of privacy issues to many transactions means that the plaintiff may have difficulty pressing a claim that he specifically relied on the express or implied privacy policies.[167] Finally, contract actions require privity of contract to have standing to assert any claim.[168] Because of the distributed and mobile nature of information, data breaches and privacy violations are often committed by third parties, such as data brokers,[169] who are not in privity with, and often not even known to, the potential plaintiff.[170] This tendency toward a lack of privity is likely part of the reason why companies are lax in their protection or discretion in storing and using personal data.[171] Especially in cases of data brokers, privity is difficult, if not impossible, to show because the subject has no contact with the collecting entity and may not even know that the broker possesses the information.

E. Quasi-Contract and Restitution

To avoid the privity problem of pure contract theories, Peek suggests using restitution as a legal method to tie the business to the subject.[172] Quasi-contract theory, unlike pure contract, does not require the bargaining, consent, and privity that has proven to be a sticking point in data privacy cases.[173] Instead, it focuses on unjust enrichment and restitution: a firm that has profited by using a subject's data must "restore the benefits" that have unjustly enriched the firm,

---

165 Sobel et al., *supra* note 9, at 56.

166 *See* Solove, *supra* note 1, at 769 (quoting Dyer v. Northwest Airlines Corp., 334 F. Supp. 2d 1196, 1200 (D.N.D. 2004) and *In re* Nw. Airlines Privacy Litig., No. 04-126 2004 WL 1278459 (D. Minn. June 6, 2004)).

167 *See id.*

168 *See* RESTATEMENT (SECOND) OF CONTRACTS, § 309 (1979).

169 *See infra* Part II.D; *see* PEEK, *supra* note 24, at 139.

170 Peek, *supra* note 24, at 139. For an examination of how private litigation has failed because it did not use contract law, *see* Sobel et al., *supra* note 9, at 60–63.

171 Peek, *supra* note 24, at 139.

172 *Id.* at 140–47.

173 *Id.* at 153, n.61 (quoting Univ. of Colorado Found. v. Am. Cyanamid Co., 342 F.3d 1298, 1309 (Fed. Cir. 2003) (citation omitted); DCB Constr. Co. v. Cent. City Dev. Co., 965 P.2d 115, 119 (Colo. 1998) (stating that unjust enrichment causes of action arise "not from consent of the parties, as in the case of contracts expressed or implied in fact, but from the law of natural immutable justice and equity.")).

if that profit has come at the expense or exposure of the subject.[174] While the idea that the subject has a property right to their personal data is a novel approach,[175] quasi-contract does not require that the subject be dispossessed of any property or even have a right in it.[176] Rather, in restitution, the benefit and the harm are separate and do not rely on one another, a disjunction particularly well-suited to the world of personal data, which exists in many places simultaneously.[177]

Quasi-contract, however, is not a conclusive solution. Like tort approaches, quasi-contract suits suffer from a difficulty of valuation. Even if the court is prepared to accept that the enrichment is unjust, such as in cases where misuse, mishandling, or loss of the data has disadvantaged the plaintiff, the actual value of this enrichment is difficult to show.[178] In fact, compared to tort damages that can, at a minimum, be grounded in the need to pay for identity theft protection and credit reports, restitution damages are unhelpfully amorphous. The courts that dismissed *Guin* and *Randolph* are unlikely to be any more receptive to claims of damages based on the increased threat of identity theft or nebulous harm of "information alienation."[179]

F. Piecemeal Protection: The Need for Something More

The largest problem facing common law approaches to data privacy problems is the amorphous nature of privacy itself. As discussed, "the concept of 'privacy' [is] . . . too vague and unwieldy a concept to perform useful analytical (and hence, legal) work."[180] The intuitive concepts of fairness and reciprocity do not naturally map onto the legal requirements of duty and tangible damages. A right of audit is a legally and practically feasible way to begin tying these concepts together to better translate the abstract concept of "privacy" into specific legal interests that the law can deal with and protect more readily.

---

[174] *See* Burlington N. R.R. Co. v. Sw. Elec. Power Co., 925 S.W.2d 92, 97 (Tex. App. 1996); *see also* Interform Co. v. Mitchell, 575 F.2d 1270, 1278 n.4 (9th Cir. 1978) (*quoted in* Peek, *supra* note 24, at 150, n.30) ("[I]n unjust enrichment [cases] . . . the recovery granted is not based upon a contract and . . . the underlying standard for the recovery is the net benefit conferred upon the defendant.").

[175] *See* Corien Prins, *Property and Privacy: European Perspectives and the Commodification of our Identity*, *in* THE FUTURE OF THE PUBLIC DOMAIN: IDENTIFYING THE COMMONS IN INFORMATION LAW 224–25 (Lucie Guibault & P. Bernt Hugenholtz eds., 2006) (noting little discussion of such a proposed right outside of the United States).

[176] *See* Peek, *supra* note 24, at 141.

[177] *See infra* notes 201 and 202.

[178] Peek, *supra* note 24, at 143–45 (noting that valuation of enrichment is complicated by the potential for significant asymmetry between the benefit to the defendant and the loss to the plaintiff).

[179] *See id.* at 138.

[180] *See* WACKS, *supra* note 3, at 10–11.

V. PRIVATE RIGHT OF AUDIT

A. A Look in the Books – Right of Audit Defined

A right of audit is a discrete, limited responsibility of the data holder to the subject of that data.[181] It does not give the subject a property interest in the data, or limit what the collector can do with the information—consistent with the American view of information as being the result of the work of the collector and thus the collector's property.[182] What a right of audit does do is set a minimum level of accountability in the form of disclosure that the information exists, what it consists of, how it was collected, and how it is being used.

Essentially, a right of audit is a way to give legal force to the important, but non-legal, concept of fairness that is offended when personal information is alienated from the person it concerns.[183] The recurring use of "fair" in the privacy law context hints at this goal as an underlying motivation for much of the privacy principles and legislation already in existence.[184] The most notable and well established right of audit is incorporated into the Fair Credit Reporting Act,[185] and the Fair Information Practice Principles are the guiding document on the subject at the FTC.[186] Fairness, in the collection of personal information, dictates that the subject of the collection have at least as much information as the entity collecting it. This basic premise gives rise to three component rights that should be considered in crafting an effective right of audit: (i) Access, (ii) Correct/Annotate/Delete, and (iii) Source/Distribution.

---

[181] The right of audit is analogous to the OECD's "Individual Participation Principle" which the OECD Expert Group recognized as "[not] . . . absolute," but nonetheless "clear and specific." ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT, OECD GUIDELINES ON THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF INFORMATION 43 (2002), *available at* http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html.

[182] *See Your Vanishing Privacy*, *supra* note 21; Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 HARV. L. REV. 2055, 2056–57 (explaining that American companies view personal data as a corporate asset). The proposed right of audit deliberately stops short of establishing an individual's ownership right in the data, a premise which, taken to its logical conclusion, "would almost certainly produce a citizenry that spends half the next century in courtrooms . . . to keep other people from sharing this or that snippet of knowledge without permission. . . ." David Brin, THE TRANSPARENT SOCIETY: WILL TECHNOLOGY FORCE US TO CHOOSE BETWEEN PRIVACY AND FREEDOM? 91 (1998).

[183] 153 CONG. REC. S1628 (daily ed. Feb. 6, 2007) (statement of Sen. Leahy).

[184] *See supra* Part II.B.

[185] *See* Fair Credit Reporting Act, 15 U.S.C. 1681i(a)(1)(A) (2006).

[186] FED. TRADE COMM'N., PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE 17–18 (2000).

B. Access

The general idea of a right of review is not controversial.[187] It is almost universally accepted by both government and private entities and is incorporated into federal and state law, as well as private business practices.[188] Differences in implementation, however, can result in widely differing effectiveness. The Transportation Security Administration's ("TSA") Traveler Redress Inquiry Program ("TRIP") requires that individuals show a specific grievance in order to access the TSA's audit procedures.[189] Credit reporting agencies are only required to allow consumers to check their credit report annually without charge.[190] Finally, the right of audit proposed in the Data Privacy and Security Act of 2009 was restricted to data brokers and would not have included companies that nonetheless have substantial amounts of personal information, such as ISPs and private companies who purchase consumer information from data brokers.[191] Additionally, the Personal Data Privacy and Security Act of 2009 would allow brokers to charge subjects a fee to access their own data.[192] Such details could greatly affect the actual ability of a right of review to effectively inform individuals. Part VI below examines these implementation details and provides several recommendations.

The right of review alone, however, is as ineffective as it is uncontroversial.[193] Merely being aware of the contents of a dossier provides little comfort or help to an individual troubled by potential inaccuracies or misuses of that information. Review is the critical first step, but in order to be effective, it must be supported by ways in which the individual can respond to the information

---

[187] *See generally supra* Part III.E.

[188] *See generally supra* Part III.

[189] U.S. Department of Homeland Security, Activities and Programs, DHS Traveler Redress Inquiry Program, http://trip.dhs.gov/ (last visited Oct. 4, 2009) (providing a limited selection of grievances that TRIP is intended to address).

[190] Fair and Accurate Credit Transactions Act of 2003, 15 U.S.C. § 1681j(a)(1)(A) (2006).

[191] Personal Data Privacy and Security Act of 2009, S. 1490, 111th Cong. § 201(c)(1). Section 3(5) defines a "data broker" as:

> a business entity which for monetary fees or dues regularly engages in the practice of collecting, transmitting, or providing access to sensitive personally identifiable information on more than 5,000 individuals who are not the customers or employees of that business entity or affiliate primarily for the purposes of providing such information to nonaffiliated third parties on an interstate basis.

S. 1490, § 3(5).

[192] S. 1490, § 201 (stating that "[a] data broker shall, upon the request of an individual, disclose to such individual for a reasonable fee all personal electronic records pertaining to that individual").

[193] Like the data-breach notification rules, a bare right of access could become less of a tool for consumers to manage their personal information and more of a tool for data holders to minimize their exposure. *Cf.* Schneier & Ranum, *supra* note 146.

he or she receives.

C. Correction, Annotation, and Deletion

An individual's right to correct or delete privately held data about themselves would seem to be a natural outgrowth of the right to review. Indeed, many of the most important codifications of privacy rights recognize the logic that a right of review is hollow without the corresponding right to act on the information.[194] But while the best practice of requiring notice and "opt in" would seem to suggest an uncontroversial ability to "opt out," the value of accurate individual records makes this less symmetrical than it appears. Because a right of correction and deletion would require a company to accept the user's modifications of the information that it has expended effort to collect, a right of correction or deletion is likely to be troubling from a business standpoint and, consequently, a legal one.[195] Companies dealing with their customers generally have contracts or user agreements that outline their information collection policies and grant the company the right to create and maintain the records.[196] A right of correction would largely conflict with the rights given to the company in such a contract. In the case of third party commercial data collectors, such as data brokers, this type of provision would be even more troublesome because the records themselves are often corporate assets.[197] Scholars have recognized that tampering with companies' rights to use this data may

---

[194] *See, e.g.,* FIPP, *supra* note 117. In addition to the U.S. government's CFIP and FIPP codifications, the right of correction is also acknowledged across the private sector and internationally. The dual rights of access and correction have been a part of many of the major data privacy initiatives, including the EU Directive on Privacy in 1995. Official Journal of the European Communities of 23 November 1995 No L. 281, Council Directive 95/46, art. 12, *available at* http://www.cdt.org/privacy/eudirective/EU_Directive.html.

[195] *See Your Vanishing Privacy*, *supra* note 21; *see* Titus, *supra* note 84 (noting that personal data is similar to property in that it has value and is fungible).

[196] *See, e.g.*, PayPal, *Privacy Policy for PayPal Services*, http://www.paypal.com/cgi-bin/webscr?cmd=p/gen/ua/policy_privacy-outside (last visited Sept. 4, 2009) ("This policy describes the ways we collect, store, use and protect your personal information. You accepted this policy when you signed up for our Service."); Facebook, *Privacy Policy*, http://www.facebook.com/policy.php (last visited Sept. 4, 2009) ("By using or accessing Facebook, you are accepting the practices described in this Privacy Policy.").

[197] Schwartz, *supra* note 182, at 2056–57; *Your Vanishing Privacy*, *supra* note 21; *see also* Twitter, *Twitter Privacy Policy*, http://twitter.com/privacy (last visited Sept. 4, 2009). Twitter's privacy policy provides:

> Twitter may sell, transfer or otherwise share some or all of its assets, including your personally identifiable information, in connection with a merger, acquisition, reorganization or sale of assets or in the event of bankruptcy. You will have the opportunity to opt out of any such transfer if the new entity's planned processing of your information differs materially from that set forth in this Privacy Policy.

Id.

violate the property interest that the company has in its work product and also represent a potential loss of the value of the asset.[198] Thus, while a right of correction or deletion has a certain logic to it and appeals to the individual-as-owner model recognized in German law,[199] such a provision could be highly burdensome and legally objectionable as a regulatory taking under the Fifth Amendment.[200]

An alternative to correction, employed by the Australian government via its National Privacy Principles, is annotation, which would allow the subject to provide his own information.[201] While annotation does not go as far as correction and deletion in giving the subject control over his data, it is attractive because it avoids the taking problem and could therefore be more palatable to businesses and constitutional lawyers.

D. Source and Distribution

An inherent characteristic of digital data is its ease of distribution.[202] Once

---

[198] Vera Bergelson, *It's Personal but is it Mine? Toward Property Rights in Personal Information*, 37 U.C. DAVIS L. REV. 379, 440 (2003) (citing Fred H. Cate, *The Changing Face of Privacy Protection in the European Union and the United States*, 33 IND. L. REV. 173, 207 (1999) (expressing concern that "[i]f the government prohibits the processing of personal data, it could deny the owner all or most of the 'economically viable use' of that data.")).

[199] *See* Thomas R. Klötzel, *Germany*, *in* INTERNATIONAL PRIVACY, PUBLICITY AND PERSONALITY LAWS 164 (Michael Henry ed., 2001) (providing a brief overview of Germany's Federal Data Protection Act of 1991, which vindicates an individual's "general personality right" to be protected against unlimited collection, use, and dissemination of personal data by both the government and private sector entities).

[200] U.S. CONST. amend. V ("No person shall . . . be deprived . . . [of] property, without due process of law; nor shall private property be taken for public use, without just compensation."); Bergelson, *supra* note 198, at 440.

[201] Privacy Act, 1988, § 14 (Aus.), *available at* http://www.comlaw.gov.au/ComLaw/Legislation/ActCompilation1.nsf/0/ABDE256E05DF7DD6CA2576080018DAE4/$file/Privacy1988_WD02.pdf.

> Where: (a) the record-keeper of a record containing personal information is not willing to amend that record, by making a correction, deletion or addition, in accordance with a request by the individual concerned . . . the record-keeper shall, if so requested by the individual concerned, take such steps . . . as are reasonable in the circumstances to attach to the record any statement provided by that individual of the correction, deletion or addition sought.

Id.

[202] Daniel J. Solove, *Access and Aggregation: Public Records, Privacy and the Constitution*, 86 MINN. L. REV. 1137, 1152 (2002); *see also* Simson Garfinkel, *Separating Equifax from Fiction*, WIRED, Sept. 1995, at 96, *available at* http://www.wired.com/wired/archive/3.09/equifax.html (citing Columbia University Professor Alan Westin's statements that "[a]lmost inevitably, transferring information from a manual file onto a computer triggers a threat to civil liberties, to privacy, to a man's very humanity because access is so simple").

information has begun to be disseminated on the Internet or through the network of data aggregators, it is extremely difficult to identify the original source and the extent of the distribution.[203] Affiliate sharing programs,[204] whereby data brokers purchase databases (or even whole companies),[205] as well as sales of customer records as assets, can quickly propagate an individual's data throughout the information ecosphere.[206] Neither the right of review nor the right of correction has any real force if the subject cannot identify the source or recipient of the information that he or she is reviewing. The Personal Data Privacy and Security Act of 2009 acknowledges this concept peripherally,[207] but the language of the Act contains an important misstep with regard to information disclosure. Specifically, under section 201(d), data brokers would be required to disclose to those individuals who have had their data breached by third parties, at no-cost to the individual, the identity of the providing broker, the identity of the requesting entity, and a copy of the information itself.[208] Although the requirement of active disclosure and identification of the providing and requesting parties is laudable, the language is both too vague and too underinclusive to provide a model for an effective right of review. It is too vague in that it does not define "adverse actions." Even if it did, such an attempt would be largely futile since the uses of information are as diverse as the information itself, and a legislature would be hard pressed to craft a definition that encompassed all the adverse uses to which an individual's data could be put. More importantly, the adverse actions disclosure would only apply when an adverse action is actually taken by a third party.[209] In contrast to these weak protections, a better model for protecting individuals can be found in the Fair Credit Reporting Act, which allows individuals to see who has accessed their information whether or not any action was taken.[210]

---

[203] JONATHAN ZITTRAIN, THE FUTURE OF THE INTERNET—AND HOW TO STOP IT 226 (2008) (contrasting current data practices in the context of the hypertext-based Internet with that of sociologist and information technology futurist Theodor Nelson's idea of dynamically linked "transclusion" that would make subsequent references dependent on the original source).

[204] *See* Hoofnagle, *supra* note 37.

[205] *See* Harris, *supra* note 26 (observing that as of 2004, data broker ChoicePoint has purchased forty-two companies, some of which it bought to acquire the data they owned).

[206] *See Your Vanishing Privacy*, *supra* note 21.

[207] Personal Data Privacy and Security Act of 2009, S. 1490, 111th Cong. (2009).

[208] S. 1490, § 201(d).

[209] S. 1490, § 201(d). Section 201(d) specifies that "if a person takes any adverse action [they] . . . shall provide [notice]". This means that the action is complete before notification is made.

[210] 15 U.S.C. § 1681j.

VI. IMPLEMENTATION

In addition to the component rights of the right of audit, there are more procedural implementation issues that will make a big difference in how effective the right is operationally. Taking a cue from the strengths and weakness of other legislative actions such as the FCRA and the Freedom of Information Act ("FOIA"),[211] what follows is a pragmatic analysis of how to best ensure that the components discussed in Part V, (Review, Correction/Annotation/Deletion, Determine, and Source and Distribution) are packaged so as to be deployed effectively. A review of the development of the FCRA and the FOIA, supplemented by other pertinent cases, will illustrate four procedural components that are vital to the viability of the proposed statute and its effectiveness upon coming into force. The law must: a) be discrete and "swallowable" so that it can move through the legislative process; b) apply broadly and not be limited only to data brokers; c) be procedural and not substantive; and d) not pre-empt state laws.

A. "Swallowable"

Professor Wacks' statement that the "false god of privacy" should be avoided[212] meant that legislators and policy makers should not attempt to establish or protect an amorphous "right of privacy" but should instead establish and protect those rights that contribute to a state of being that better accords with the important, but non-legal, notion of privacy.[213] In essence, start small.

While Bruce Schneier and other privacy advocates push for broader and more comprehensive privacy laws,[214] a single, discrete principle with clear implications and a straightforward implementation is a more effective route forward at this time when increasing obvious need meets increasingly conspicuous inaction.[215] It is often easier to build on an existing right than to create one

---

[211] The Freedom of Information Act, 5 U.S.C. § 552 (2007). In recommending the FOIA legislation for adoption, the Senate Committee on the Judiciary reported that it "would establish a much-needed policy of disclosure. . . ." S. REP. NO. 813, at 10 (1965) The House agreed, finding that it would provide the "machinery to assure the availability of Government information necessary for an informed electorate." H.R. REP. NO. 1497, at 12 (1966), *reprinted in* 1966 U.S.C.C.A.N. 2418, 2429.

[212] WACKS, *supra* note 3, at 10.

[213] *See id.* (referencing American legal scholar R.F. Hixson's argument that legislation should "regulate clearly identified threats to sensitive information" (citing R.F. HIXSON, PRIVACY IN A PUBLIC SOCIETY: HUMAN RIGHTS IN CONFLICT 98 (1987))).

[214] *See, e.g., Our Data Ourselves*, *supra* note 11.

[215] 153 CONG. REC. S1628 (daily ed. Feb. 6, 2007) (statement of Sen. Leahy) (referring to the irony of Congressional leadership refusing to address the 2006 version of the Personal Data Privacy and Security Act even as reports of data breaches and identity theft continued at alarming levels).

from scratch. This is the lesson of the FOIA, which was largely toothless at its inception but was significantly enhanced after Watergate, when the need for accountability became more evident.[216] Development of frameworks to handle expansive and amorphous problems is best approached as an iterative task, whether it be designing widgets or forming the European Union.[217] To avoid policy paralysis, it is better to take a small first step than to continue the pattern of comprehensive and ideal, but ultimately unsuccessful, legislative initiatives.

B. Broadly Applicable

To be effective, a right of review must reach all those entities that keep records that, if misused, stolen, or lost, could affect the individual. In this respect, the demographic, transactional, and public records information held by data brokers is less of an issue than substantive information such as purchasing history information on eBay or the Web search information held by search engines and ISPs.[218] Despite its strong steps in the right direction, S. 1490 errs because it is limited only to "data brokers," a restrictive definition as defined in the legislation.[219] The language of S. 1490 specifically leaves out affiliate sharing programs and in-house data mining operations like Kroger Corporation's DunnhumbyUSA,[220] and does not even contemplate applying to corporations as a whole.[221]

---

[216] Alan F. Westin, *Information, Dissent, and Political Power, in* WATERGATE AND AFTERWARD: THE LEGACY OF RICHARD M. NIXON 59 (Leon Friedman & William F. Levantrosser eds., 1992). Initially, the Freedom of Information Act of 1966, Pub. L. No. 89-487, § 3, 80 Stat. 250 (1966), lacked explicit procedural requirements such as public indices of agency information, timeframes for agency action on FOIA requests, recovery of reasonable attorney fees, or annual reporting on the administration of FOIA. Congress later modified the act to address these shortcomings, Pub. L. No. 93-502 (b)(1)P.L. 93-502 (1974) (codified as amended at 5 U.S.C. § 552 (2006)).

[217] *See, e.g.,* Video: David Kelley, *Design as an Iterative Process* (Oct. 10, 2001), *available at* http://academicearth.org/lectures/design-as-an-iterative-process ("How quickly you get to the first crummy prototype . . . is directly proportional . . . to how successful the product will be."); *see also* JEREMY JOHN RICHARDSON, EUROPEAN UNION: POWER AND POLICY MAKING 42 (2006) (characterizing treaty reform and European Union integration as an iterative process which is the result of "incremental, institutional adjustments . . . .").

[218] *See* Omar Tene, *What Google Knows: Privacy and Internet Search Engines*, UTAH L. REV. 1433, 1441–45 (2008). While data breaches have only an attenuated risk of financial harm, AOL's disclosure of Web search records had a much more immediate impact on the lives of its customers. *Id.* at 1443–44. Additionally, last year, a federal judge ordered Google to provide Viacom twelve terabytes of data on viewers of its YouTube Web site. Viacom Int'l Inc. v. YouTube, Inc., Nos. 07 Civ. 2103(LLS), 07 Civ. 3582(LLS), 2008 WL 2627388, at *5 (S.D.N.Y. July 2, 2008). The records included un-obfuscated IP addresses and time stamps that together effectively create a personally identifiable viewing history. *Id.*

[219] Personal Data Privacy and Security Act of 2009, S. 1490, 111th Cong. § 201 (2009).

[220] *See* Sewell, *supra* note 16 and accompanying text.

[221] *See* S. 1490, § 201.

C. Procedural, Not Substantive

The rules that provide a framework for privacy protection can be procedural: addressing *how* personal information is collected and used by governing the methods by which data collectors and data providers interact.[222] Alternatively, the rules can be substantive, governing *what* can be collected and what it can be used for.[223] While many countries include substantive limits on the types of data that can be collected and their permissible uses,[224] such fine-grained decisions would needlessly hamstring this proposed legislation. Procedural rules are better suited to early action because they are more straightforward in implementation and implications. Moreover, the experience gained under the procedural rules can help shape more effective and better tailored substantive rules if and when they become appropriate.[225]

D. No Federal Pre-Emption

One of the great values of having multiple jurisdictions is the opportunity to experiment. While data brokers like LexisNexis argue for federal preemption as a way to avoid "struggling with complying with multiple potentially conflicting and inconsistent state laws,"[226] federal preemption would in fact be counterproductive to advances in both consumer privacy and pro-business privacy law innovation.[227] Inconsistencies in state law are often the vanguards of

---

[222] *See, e.g.*, Aaron J. Burstein, *Amending the ECPA to Enable a Culture of Cybersecurity*, 22 HARV. J.L. & TECH., 168, 208 (2008) (highlighting HIPAA Privacy Rules as an instructive model possessing both procedural and substantive elements).

[223] *See, e.g., id.*

[224] *See* GUTWIRTH, *supra* note 78, at 87 (tracing the occurrence of substantive limits on data collection and use from the OECD framework back at least forty years to the French "Law Relative to Computer Science, to Records, and to Liberties"); *see also id.* at 119 (providing that Article eight of the 1995 European Community directive on the "processing of personal data," provides substantive restrictions on "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."). *See generally* INTERNATIONAL PRIVACY, PUBLICITY, AND PERSONALITY LAWS (Michael Henry, ed. 2001) (providing summary overviews of the privacy and data protection laws of twenty-nine countries).

[225] The version of the FOIA that President Johnson signed into law was principally substantive without a procedural framework. *See* Westin, *supra* note 216 and accompanying text. Ultimately, either approach would satisfy the "first step plus iterations" approach urged by Kelley. *See* Kelley, *supra* note 217. Of the two, the procedural-first "if you build it, they will come" approach seems more likely to be effective.

[226] *Securing Electronic Personal Data: Striking a Counterbalance Between Privacy and Commercial and Government Use: Hearing Before the S. Comm. On the Judiciary*, 109thg Cong. 11–12 (2005) (statement of Kurt P. Sanford, President & CEO, U.S. Corporate and Fed. Gov. Markets, LexisNexis).

[227] *See* Solove, *supra* note 96, at 117 (characterizing the federal pre-emption element of the FACTA as significantly undercutting the Act's benefits by preempting more protective

important policy change and legal innovation, as evidenced by California's breach notification law that helped lead to the large scale media interest and ensuing public pressure following the 2005 ChoicePoint incident.[228] Because of the disclosure requirements, the breach drew national attention to California's then unique law which ultimately served as the template for breach notification laws that have since been adopted nationwide.[229] A patchwork, state-by-state approach is not only feasible for data holders, it is the status quo for much of privacy law.[230] It also benefits the consumer and the data holder because it creates a market of ideas where effective legal innovation is adopted and standardized.[231] Despite industry concerns, like those voiced by LexisNexis,[232] preemption cuts both ways: it provides states the opportunity to come up with ways are ultimately pro-business, but which would run afoul of one-size-fits-all federal preemption.[233] The potential for this sort of pro-business/pro-consumer innovation is illustrated by a 2008 California bill that would have allowed differential insurance premiums for drivers who opt for an automobile black box and significant savings, instead of privacy.[234] The Sarbanes-Oxley

---

state statutes).

228 *See id.* at 112.

229 SYNOVATE, FED. TRADE COMM'N - 2006 IDENTITY THEFT SURVEY REPORT 55 n.45 (2007), *available at* http://www.ftc.gov/os/2007/11/SynovateFinalReportIDTheft2006.pdf (explaining that "[s]ince the passage of the California statute, over 30 other states have passed some form of breach notice law."); *see also* Walden, et al., *supra* note 116 (noting that the California statute has "served as a model for many other states").

230 *See* Chander, *supra* note 140, at 3 (describing the current state of privacy law as "cobbled together from a disparate array of federal statutes, a few state laws, and common law . . . . [with] no overarching framework, but rather episodic privacy protections for limited domains and in certain circumstances."). For most large corporations, variations in the law from state to state pale in comparison to the variation in international privacy law. *Compare, e.g.,* Acxiom, Global Privacy Principles, http://www.acxiom.com/about_us/privacy/Pages/Privacy.aspx (last visited Sept. 2, 2009) (describing general policy principles); *with* Acxiom, Highlights for U.S. Products Privacy Policy, http://www.acxiom.com/about_us/privacy/consumer_information/highlights_for_US_product_privacy_policy/Pages/HighlightsforUSProductsPrivacyPolicy.aspx (last visited Sept. 2, 2009) (detailing privacy policies specific to the U.S. market).

231 *See* New State Ice. Co. v. Liebmann, 285 U.S. 262, 311 (1932) (Brandeis, J., dissenting) (describing the federal system as allowing "a single courageous state . . . to serve as a laboratory; and try novel social and economic experiments without risk to the rest of the country.").

232 *Securing Electronic Personal Data: Striking a Counterbalance Between Privacy and Commercial and Government Use: Hearing Before the S. Comm. On the Judiciary*, 109th Cong. 11–12 (2005) (statement of Kurt P. Sanford, President & CEO, U.S. Corporate and Fed. Gov. Markets, LexisNexis).

233 *See generally* Paul M. Schwartz, *Preemption and Privacy*, 118 YALE L.J. 902 (2008) (discussing the benefits and drawbacks of federal preemption in the area of privacy legislation). Schwartz concludes that a "federal omnibus information privacy law" . . . "would limit further experimentation in federal and state sectoral laws." *Id.* at 946.

234 A.B. 2800, 2008 Assem., Reg. Sess. (Cal. 2008).

Act,[235] adopted in response to major corporate accounting scandals,[236] is an example of legislation that is intended to set a federal baseline protection that does not preempt state law and can be improved upon if a state desires.[237]

E. Central Clearinghouse for Requests

Finally, to both simplify administration and reduce the costs imposed on private data holders, a federal right of audit should be accompanied by provisions for the creation of a central clearinghouse for audit requests. This clearinghouse would most naturally fit under the auspices of the FTC's Bureau of Consumer Protection, which currently manages a similar data protection program for victims of identity theft.[238]

Such a clearinghouse has precedent and has served as a model for several successful federal and private-sector programs.[239] Perhaps the closest analogue to the proposed clearinghouse is the constellation of "nationwide consumer credit reporting agencies" that developed in response to the "free annual disclosure" provisions of the FACTA.[240] While AnnualCreditReport.com, the official, centralized source of free credit reports created by Equifax, Experian and TransUnion, is the best known result of FACTA's provisions, provisions of FACTA also apply to myriad smaller players across a variety of industries, such as the Medical Information Bureau[241] (provider of medical records) and ChoicePoint's C.L.U.E. service (provider of insurance reports).[242] Interestingly, the FTC has repeatedly declined to publish a list of companies that qualify as "nationwide specialty consumer reporting agencies."[243] This shortcoming in implementation of the FACTA illustrates how a national clearinghouse could

---

[235] Sarbanes-Oxley Act of 2002, Pub. L. No. 107-204, 116 Stat. 745 (codified in scattered sections of 11, 15, 18, 28, and 29 U.S.C.).

[236] Rob Norton, *The Cure for Lavish Pay? Shame It to Death*, WASH. POST, Sept. 29, 2002, at B1.

[237] *See* Sarbanes-Oxley Act of 2002, Pub. L. No. 107-204, § 303(c), 116 Stat. 745 (stating that "[t]he provisions of subsection (a) shall be in addition to, and shall not supersede or preempt, any other provision of law or any rule or regulation issued thereunder.").

[238] *See* Fed. Trade Comm'n., Division of Privacy and Identity Protection, http://www.ftc.gov/bcp/bcppip.shtm (last visited Sept. 4, 2009).

[239] *See, e.g.*, Federal Trade Comm'n, National Do Not Call Registry, http://www.ftc.gov/donotcall (last visited Oct. 7, 2009).

[240] *See* Annual Credit Report, *About Us*, https://www.annualcreditreport.com/cra/helpabout (last visited Sept. 20, 2009).

[241] *See* MIB Group, New Breed of Identity Crime: Medical Identity Theft, http://www.mib.com/html/medical_id_theft.html (last visited Sept. 4, 2009).

[242] *See* LexisNexis ChoicePoint, FACT Act, http://www.choicepoint.com/factact.html (last visited Sept. 4, 2009).

[243] Privacy Rights Clearinghouse, Facts on FACTA: The Fair and Accurate Credit Transaction: Consumers Win Some, Lose Some, http://www.privacyrights.org/fs/fs6a-facta.htm#8 (last visited Sept. 4, 2009).

help translate the will for change into actual gains for the consumer.

VII. CONCLUSION

Privacy may be difficult to define, but privacy rights are ultimately quite straightforward. By avoiding the temptation to reach for all-encompassing definitions or comprehensive statutes, a simple initiative can begin to succeed where more ambitious efforts have repeatedly failed. The right of audit, while narrowly circumscribed, does not continue the unfortunate trend of haphazard, piecemeal protection that has often characterized previous statutory efforts. Instead, it vindicates a small constellation of discrete rights across all actors and industries, in keeping with the tradition of the more successful formulations of privacy rights.[244] While the important but amorphous value of privacy certainly deserves more than this rudimentary protection, it must be recognized that addressing complex problems is an iterative process.[245] Legislators and policy makers should acknowledge that the growing importance of data privacy policy means that something must be done, and that now is not the time to let perfect be the enemy of good.[246]

APPENDIX: EXAMPLE STATUTE

The following text provides simplified statutory language to illustrate how a right of audit might be implemented.

An Act

To authorize the Federal Trade Commission to implement and enforce a "Right of Audit" in data held by private entities and to create a "Consumer Information Clearinghouse" to administer the program.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

---

244 *See* Section II.B.

245 *See* Kelley, *supra* note 217.

246 *See* VOLTAIRE, LA BÉGUEULE (1772).

SECTION 1: INTRODUCTION[247]

1.1 Congress finds that—

(a) databases of personally identifiable information are a powerful resource which play a fundamental role in the convenience, accuracy, speed, and power of commerce and communication in a computer-mediated society;[248]

(b) the extraordinary power of these databases means that:

(i) insecure and unreliable information management creates risks from threats both malicious and systemic which have the potential to disrupt and undermine the livelihood, liberty, confidence and privacy of Americans as well as compromise the efficiency and effectiveness of business and government operations;

(ii) secure and reliable databases are integral to the advancement of national priorities such as economic stability, national security, the continued development of e-commerce, and the privacy rights of Americans;

(c)because governmental use of commercial databases of personally identifiable information affects the critically important areas of individual privacy and national security, Congress must provide for oversight of the use of these databases; and

(d) "individuals whose personal information" is used or held by data aggregators have a legally recognized expectation of "fairness, transparency, accuracy, and respect for the privacy of consumers;"[249] *and*

(e) "therefore the foregoing reasons, data aggregators have a concomitant obligation to meet that expectation."[250]

SECTION 2: DEFINITIONS

2.1 Information Aggregator - The term "information aggregator" (herein "aggregator" or "holder") means a business entity collects personally identifiable information on more than 5,000 individuals;[251] and:

---

[247] Adapted from section 2 (Findings) of the Personal Data Privacy and Security Act of 2007, S. 495, 110th Cong. (2007).

[248] *See, e.g.*, Daniel J. Solove, THE DIGITAL PERSON 14–27 (2004), *available at* http://docs.law.gwu.edu/facweb/dsolove/Digital-Person/text/Digital-Person-CH2.pdf (chronicling the revolutionary effect of computers and digitization on public and private sector databases).

[249] S. 495, § 2(9).

[250] *Id.*

[251] The term "information aggregator" is used to differentiate the broader concept of "private entities holding extensive personal information" from the more limited term "data brokers," which has come to be used, as in S. 495, to refer only to those entities whose prin-

(a) sells, leases, or otherwise disseminates the information for a fee;[252]

(b) data mines or aggregates,

(c) purchases, trades, or acquires records from an information aggregator[253]

2.2 Personally identifiable information – Personally identifiable information is that information or combination of information which can identify a particular individual. Personal Information includes but is not limited to a person's name; biographical details, present or past addresses, contact information, identifying number or code; educational, medical, criminal history or employment history or other identifying particulars inherent or assigned to the individual, "such as a fingerprint, voiceprint, DNA, iris image, or photograph."[254]

2.3 Anonymous Information - Combinations of personal information which cannot be tied to an identifiable individual are "anonymous data" which are not covered under this statute.[255]

2.3 Data mining – The term "data mining" means the combination of self-reported or otherwise verified data about an identifiable individual to produce information that was not provided to the aggregator and not composed of facts or history, and/or is speculative, predictive, or evaluative of the character, habits, or behavior of an identifiable individual.

---

ciple business is the collection and dissemination of information. *Cf.* Personal Data Privacy and Security Act of 2007, S. 495, 110th Cong. § 3(5) (2007). The Act defines a "data broker" as

> a business entity which for monetary fees or dues regularly engages in the practice of collecting, transmitting, or providing access to sensitive personally identifiable information on more than 5,000 individuals who are not the customers or employees of that business entity or affiliate primarily for the purposes of providing such information to nonaffiliated third parties on an interstate basis.

Id.

The distinction is made clear as Solove notes:

> [P]rivacy may be implicated if one combines a variety of relatively innocuous bits of information. Businesses and government often aggregate a wide array of information fragments, including pieces of information we would not view as private in isolation. Yet when combined, they paint a rather detailed portrait of our personalities and behavior, a problem I call "aggregation."

DANIEL J. SOLOVE, UNDERSTANDING PRIVACY 70 (2008).

252 This is intended to target the "data brokers" that were the primary target of Personal Data Privacy and Security Act of 2007.

253 This targets the widespread practice of "affiliate sharing" where tenuously connected businesses cooperate to provide one another with data. *See* Hoofnagle, *supra* note 37 and accompanying text.

254 Privacy Act of 1974, 5 U.S.C. § 552(a) (2006).

255 The provision for an "anonymous information" exception is intended to permit the use of truly non-personally identifiable information in important research areas like medical research. *See, e.g.,* David Armstrong *et al, Potential Impact of the HIPAA Privacy Rule on Data Collection in a Registry of Patients With Acute Coronary Syndrome*, 165 ARCHIVES OF INTERNAL MEDICINE 1125 (2005); Jamie Heywood, *Forget Medical Privacy*, WIRED 110–11 (Oct. 2009).

2.4 Proprietary assessment – The term "proprietary assessment" means data-mining which is

(a) conducted on information pertaining to an identifiable individual who has a direct relationship with the organization; and

(b) used to produce analysis which are maintained by the organization for internal use and not sold, transferred, or otherwise disseminated.

SECTION 3: SCOPE

3.1 No requirement of consumer relationship.[256]

3.2 Excluded entities: This statute does not apply to:

(a) 501(c)(3) non-profit corporations

(b) Registered political parties

3.3 Excluded data:

(a) any data related to an individual's past purchases of consumer goods if generated by the holder of the data; or

(b) any proprietary assessment or evaluation of an individual or any proprietary assessment or evaluation of information about an individual if generated by the holder of the data.[257]

(c) any data that is not personally identifiable.

SECTION 4: RIGHT OF ACCESS[258]

4.1 Upon request, an information aggregator must provide, in an understandable form, a copy of the personally identifiable information held on the requestor unless:

(a) release of the information would unreasonably jeopardize the health, safety, or privacy of other individuals; or

(b) "the request for access is frivolous or vexatious"; or

(c) providing access would likely prejudice present or future legal pro-

---

256 This addresses the "shadow offenders" problem that has stymied contract law approaches. *See* Peek, *supra* note 24, at 139.

257 These exclusions are intended to ease the burden on entities that deal in a high volume of records but whose activities neither draw from nor contribute to the larger information ecosystem, thus minimizing their effect on the consumer. This exclusion functions as a further structural incentive for companies to self regulate, in the way that Posner found to be effective at checking the harmful effects of data aggregation in the private sector. *See* Posner, *supra* note 55, at 176 ("The government is not subject to the discipline of the marketplace which will punish a private firm or individual who demands information beyond the point where the value of the information equals the price of obtaining it.").

258 This section is adapted largely from the Australian Government's "National Privacy Principles." *See* Privacy Act, *supra* note 201.

ceedings or criminal investigations.

4.2 Charges for access are permitted if they are

(a) commensurate with the actual cost for retrieving the information; and

(b) not charged for filing the request itself.

4.3 Correction: Upon a showing that the aggregator's information pertaining to an individual is not accurate, complete and up-to-date, the aggregator must take reasonable efforts to ensure that the inaccuracy is corrected.

4.4 Annotation: In the event of a dispute as to the accuracy of information held by an aggregator, the organization must permit the individual to include an explanatory note as part of the record.

4.5: Deletion: If the individual requests the record be deleted, the organization must take reasonable measures to do so except where:

(a) the collection of the information is specifically allowed or mandated by laws applicable to both the individual and the organization;

(b) the request would be unreasonably burdensome; or

(c) the request would compromise a current or anticipated investigation, legal proceeding, or negotiation.

4.6 Denials of requests based on paragraphs 4.1(a) to (c) must consider whether the information can nonetheless be released by either

(a) redacting the protected portions; or

(b) releasing the information through an intermediary

4.7 Justification: If the organization refuses a request for access, correction, annotation, or deletion, the denial must cite the specific exception(s) invoked and explain in reasonable detail why the exception(s) applies.

SECTION 5: THE CONSUMER INFORMATION CLEARINGHOUSE

5.1 To facilitate the administration of the terms of this statute, the Consumer Information Clearinghouse shall be established under the auspices of the Federal Trade Commission.

SECTION 6: APPLICABILITY OF STATE LAW

6.1 This law does not preempt state regulation of data aggregators.

(a) Each State shall apply the provisions of this act insofar as they are not inconsistent with State law.

SECTION 7: ENFORCEMENT

7.1 Actions by private persons

(a) In general – A person or representative of a person adversely affected by data aggregation not complying with Section 4 of this Act may, "within 3 years of discovery of the violation, bring a civil action in an appropriate district court of the United States"[259] *against the aggregator.*

(b) Remedy – The remedies available for a civil action under this act include injunction to enforce compliance, monetary damages, and other relief which the court may deem appropriate.

(c) Before or immediately after bringing an action under this act, the plaintiff shall serve written notice of the action, including a copy of the complaint, upon the Commission.

The Commission shall have the right:

(a) to intervene in the action,

(b) upon so intervening, to be heard on all matters arising therein, and

(c) to file petitions for appeal."

7.3 "Actions by Commission

(a) In general – An action instituted under this Act by or on behalf of the Commission shall prevent any further private actions under this Act against any named defendants for the pendency of the action.

---

[259] 15 U.S.C. § 6104(a) (2006).