OUR WALLS IN THE INFORMATION AGE

M. Jos. Capkovic[1]

INTRODUCTION

What is privacy law? "[L]egal theorists and policy makers continue to have little idea just what our legal conception of 'privacy' is; and to the extent there is a 'law of privacy,' it remains a piecemeal, poorly understood, and only partially successful body of jurisprudence."[2] The purpose of this note is to evaluate the foundations of United States privacy law and explore whether "our own walls" are expanding in the information age.[3] It will survey the practices of commercial data brokers that collect, store, and use individuals' personal information. The analysis will review current U.S. privacy protections, and examine emerging privacy concerns--problems of "Privacy 2.0."[4] Finally, it will explore model solutions advocated by leading authorities that would serve to protect the privacy of the people of the United States in the information age.

I. THE FOUNDATION OF U.S. PRIVACY LAW

What is privacy? Is it a universal principle, or a nebulous concept that varies across cultures? In his article titled *The Two Western Cultures of Privacy: Dignity Versus Liberty*, James Whitman casts the notion of privacy as the latter.[5] Whitman identifies contemporary concepts of privacy and how they differ between the U.S. and the European continent stating: "The core continental privacy rights are rights to one's image, name, and reputation, and what Germans call the right to informational self-determination—the right to control the sorts of information disclosed about oneself."[6] Whitman continues by defining the American right to privacy as "much the form that it took in the eighteenth century: It is the right to freedom from intrusions by the state, especially in one's own home . . .maintaining a kind of private sovereignty within *our own walls*."[7]

American notions of privacy have consistently changed from the drafting of the Bill of Rights through today. Modern American notions of privacy began with the Bill of Rights. The Fourth Amendment provides that it is "[t]he right of the people to be secure in their persons,

---

[1] Fall 2011 J.D. Candidate, Regent University School of Law; B.A., Political Science, University of Missouri - Columbia. M. Jos. Capkovic is a member of the International Association of Privacy Professionals. He wishes to extend his most sincere gratitude to Professor Rebecca G. Hulse of William & Mary School of Law for her instruction and insight. His thanks also go to Professor Charles H. Oates, Ramona A. Gau, and to his wife Kelly for her support.

[2] Neil M. Richards, *The Information Privacy Law Project*, 94 GEO L.J. 1087, 1088 (2006).

[3] *See* James Q. Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 YALE L.J. 1151, 1162 (2004) (identifying the American right to privacy as maintaining a kind of private sovereignty within our own walls. Whitman is the Ford Foundation Professor of Comparative and Foreign Law at Yale Law School).

[4] JOHNATHAN ZITTRAIN, THE FUTURE OF THE INTERNET AND HOW TO STOP IT (2008), 200 (defining Privacy 2.0).

[5] Whitman, *supra* note 3, at 1151.

[6] *Id.*

[7] *Id.* (emphasis added as this note reflects upon the concept of "our own walls").

houses, *papers, and effects*, against unreasonable searches and seizures …"[8] The protections of the Fourth Amendment extend to "the people" of the U.S., not just American citizens.[9]

Nearing the end of the 19th century, Samuel Warren and Louis Brandeis wrote an article titled *The Right to Privacy*.[10] This article is widely recognized as one of the most significant law review articles ever written and is credited with helping shape U.S. privacy protections. In their article, Warren and Brandeis define privacy as a concept that includes "the right to be let alone" and "inviolate personality."[11] The article also illustrates that the challenges which emerging technologies pose to privacy are not novel. In the face of the then-recent invention of instantaneous photography, the authors voiced concern with "the too enterprising press, the photographer, or the possessor of any other modern device for recording or reproducing scenes or sounds."[12]

By 1967, it was well established that the Fourth Amendment extended beyond criminal investigations.[13] In the 1989 Supreme Court case of *Skinner v. Railway Labor Executives' Assn.*, the Court held that "[t]he [Fourth] Amendment guarantees the privacy, dignity, and security of persons against certain arbitrary and invasive acts by officers of the Government."[14] In the recent past, however, the Supreme Court appears to have avoided applying the Fourth Amendment to new technologies.[15] The court explained this phenomenon in *City of Ontario, Cal. v. Quon* stating, "The judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear."[16]

II. THE ADVENT OF THE NETWORKED COMPUTER: THE DECENTRALIZATION AND AGGREGATION OF PERSONAL INFORMATION

The advent of the "networked computer" has allowed for personal papers and effects to exist across multiple locations simultaneously.[17] The networked computer is at the center of an information age that is full of promise, but is not without dangers. Today, it appears that individuals' ability to control their personal information is being diminished by the advances of the information age.

Personal information is decentralized as data that is transmitted to and from networked computers linked to non-direct interface locations including servers and remote computer systems. Examples of such personal information include financial account information, written communications, images, and all manner of documents.

---

[8] U.S. CONST. amend. IV, (emphasis added as this note focuses upon "papers, and effects").
[9] *Id*.
[10] Samuel Warren and Louis D. Brandeis, *The Right to Privacy*, 4 HARVARD L. REV. 193 (1890).
[11] *Id*.
[12] *Id*.
[13] *See* Camara v. Municipal Court of City and County of San Francisco, 387 U.S. 523, 530 (1967).
[14] Skinner v. Railway Labor Executives' Assn., 489 U.S. 602, 613-614 (1989).
[15] *See* City of Ontario, Cal. v. Quon, 130 S. Ct. 2619, 2635 (2010) (Scalia, J., concurring in part stating: "Applying the Fourth Amendment to new technologies may sometimes be difficult, but when it is necessary to decide a case we have no choice[…]The-times-they-are-a-changin' is a feeble excuse for disregard of duty.").
[16] *Id.* at 2629 (citing how *Katz* overruled *Olmstead*).
[17] The working definition of "networked computer" for this note includes computers, tablets, smartphones, and other networked electronic devices.

Financial accounts that are commonly decentralized today include checking, savings, and credit accounts. Scores of online services and retailers (e.g., Amazon and eBay) store consumer credit card information. Written communications have likewise been decentralized in formats including email, text messaging, and social media messages. Depictions of persons (e.g., images and written accounts of persons) exist across social media and image storage services such as Facebook and Flickr. These means of decentralization highlight a significant gap between one's Fourth Amendment papers and effects as they existed in 1791 and as they exist today, in the information age.

Networked computers have allowed one to manage one's papers and effects with for greater efficiency. Processes that were typically managed in the home and carried out by telephone, post mail, or in person now take place across a series of computers (e.g., post mail versus electronic mail, and physical modes of file sharing versus digital file sharing). However, these efficiencies only exist if our computers network beyond traditional notions of our own walls. Just as the networked computer has allowed for greater efficiencies in administrating one's papers and effects, the networked computer has yielded efficiencies for the public and private sectors as well. Public and private entities have been maintaining databases on consumers for decades, and computer networking has allowed entities to provide broad access to these databases.

In his article, "Access and Aggregation," Daniel Solove addresses some problems that have arisen from the private sector's increased accessibility to public records.[18] These problems include government's "power to compel individuals to reveal a vast amount of personal information about themselves—where they live, their phone numbers, their physical description, their photograph, their age, their medical problems, all of their legal transgressions throughout their lifetimes whether serious crimes or minor infractions . . . ."[19] Solove then highlights the fact that the government routinely pours this information into the public domain by posting it on the Internet. Although he concedes that most public records are "relatively innocuous," Solove argues "it is the totality of the information, aggregated together, that presents the problem."[20] According to Solove,

> Consolidating various bits of information, each itself relatively unrevealing, can, in the aggregate, begin to paint a portrait of a person's life . . . a 'digital biography.' A growing number of private sector organizations are using public records to construct digital biographies on millions of individuals. . . .These uses are resulting in a growing dehumanization, powerlessness, and vulnerability for individuals.[21]

The decentralization and aggregation of personal information in this context has given rise to problematic uses of databases.

A. Problematic Database Applications

In their article, "A Model Regime of Privacy Protection," Solove and Chris Jay Hoofnagle note, "the privacy protections in the United States are riddled with gaps and weak spots. . . . In

---

[18]. *See* Daniel J. Solove, *Access and Aggregation*, 86 MINN. L. REV. 1137 (2002) (Solove is the John Marshall Harlan Research Professor of Law at the George Washington University Law School).
[19]. *Id.* at 1138.
[20]. *Id.* at 1141
[21]. *Id.*

particular, emerging companies known as 'commercial data brokers' have frequently slipped through the cracks of U.S. privacy law."[22] "An entire industry" has emerged that deals in the collection, processing, and dissemination of individuals' personal information, and it "is not well-regulated."[23] This section will highlight several database applications effectuated by commercial data brokers.

In his book *The Limits of Privacy*, Amitai Etzioni posits that most privacy threats that fail to serve the common good arise "not from the state, the villain that champions of privacy traditionally fear the most, but rather from the quest for profit by some private companies."[24] Etzioni casts government intrusions upon privacy as necessary when balanced against a significant "common good" (e.g., drug testing those responsible for the lives of others—such as public transportation drivers).[25] He defines the "common good" as public safety and public health.[26] "[W]hen courts and common parlance cite 'the public interest,' very often the reference is to matters that fall into one of these two pivotal categories."[27]

According to Etzioni, "corporations now regularly amass detailed accounts about many aspects of the personal lives of millions of individuals, profiles of the kind that until just a few years ago could be compiled only by the likes of . . . major state agencies, with huge staffs and budgets."[28] Etzioni concludes his thoughts on what he has termed the privacy paradox by noting,

> Although our civic culture, public policies, and legal doctrines are attentive to privacy when it is violated by the state, when privacy is threatened by the private sector our culture, policies, and doctrines provide a surprisingly weak defense. Consumers, employees, even patients and children have little protection from marketers, insurance companies, bankers, and corporate surveillance.[29]

The people of the U.S. do not enjoy any fundamental protections against unreasonable searches and seizures of their Fourth Amendment papers and effects by non-state actors. Additionally, the Supreme Court has not ruled on how it will review regulations "placed on personal information . . . used . . . in a commercial context."[30] Commercial data brokers have capitalized upon these gaps by selling individuals' personal information to the government for law enforcement purposes, to companies for marketing, to creditors for credit checks, and to employers for background checks.[31]

---

[22]. Daniel J. Solove & Chris Jay Hoofnagle, *A Model Regime of Privacy Protection*, 2006 U. OF ILL. L. REV. 357, 357 (2006).
[23] *Id.* at 359.
[24] AMITAI ETZIONI, THE LIMITS OF PRIVACY 9–10 (1999), (Etzioni is a former Thomas Henry Carroll Ford Foundation Professor of Harvard Business School).
[25] *Id.* at 3.
[26] *Id.* at 3–4.
[27] *Id.* at 4.
[28] *Id.* at 10.
[29] *Id.*
[30] Sarah Ludington, *Reining in the Data Traders: A Tort for the Misuse of Personal Information*, 66 MD. L. REV. 140, 176 (2006).
[31] *See Id.*

Commercial data brokers enjoy access to individuals' personal information collected by the government that they either cannot collect or it would be impracticable for them to collect (e.g., the cost prohibitive nature of door-to-door canvassing, which ensures the extensive sampling and robust nature of census data). Under the Privacy Act of 1974 ("Privacy Act"), government agencies are limited in the personal information they can keep.[32]

The Privacy Act provides that government agencies can maintain only individuals' personal information that is directly linked to the agency's purpose.[33] Once individuals' information is in the public sphere, however, commercial data brokers can compile it as they see fit and sell the information to the otherwise limited government agencies. The Privacy Act "restricted the government from building databases of dossiers unless the information about individuals was directly relevant to an agency's mission. Of course, that's precisely what ChoicePoint, LexisNexis, and other services do for the government."[34]

B. Governmental Applications and the Commercial Data Broker Paradox

Current gaps in the Privacy Act allow government agencies to leverage the services of commercial data brokers. In his article titled "Big Brother's Little Helpers: How ChoicePoint and Other Commercial Data Brokers Collect, Process, and Package Your Data for Law Enforcement," Chris Jay Hoofnagle states:

> This limitation to the Privacy Act is critical—it allows [commercial data brokers] to amass huge databases that the government is legally prohibited from creating. Then, when the government needs the information, it can request it from the [commercial data broker]. At that point, the personal information would be subject to the Privacy Act, but law enforcement and intelligence agencies have special exemptions under the Act that limit access, accuracy, and correction rights.[35]

Apart from the government use of private sector databases, some legal authorities have criticized the oft-employed metaphor of George Orwell's "Big Brother."[36] According to Neil Richards, "Big Brother improperly characterizes the problem of private-sector databases because marketers are not interested in authoritarian control but with the more mundane goal of selling products to consumers."[37] Yet, Orwell's all seeing state characterized by Big Brother appears to be a fitting metaphor for government data mining activities such as those exemplified by the Department of

---

[32] ROBERT O'HARROW, NO PLACE TO HIDE 137 (2005) (commenting on the Privacy Act of 1974, 5 U.S.C. § 552(a)).
[33] *Id.*
[34] *See Id.* at 137 (commenting on the Privacy Act of 1974, 5 U.S.C. § 552a).
[35] Chris Jay Hoofnagle, *Big Brother's Little Helpers: How ChoicePoint and Other Commercial Data Brokers Collect, Process, and Package Your Data for Law Enforcement*, 29 N.C.J. Int'l L. & Com. Reg. 595 (Summer 2004) (Hoofnagle is the associate director of the public interest research entity known as Electronic Privacy Information Center ("EPIC")).
[36] *See* Richards *supra* note 2, at 1091.
[37] *Id*.

Defenses' Total Information Awareness program ("TIA").[38] TIA has been cited as the classic example of "large-scale data mining."[39] It combed databases for information on "credit-card purchases, tax returns, driver's license data, work permits, travel itineraries, and other digital sources."[40]

i. Data Mining

Data mining is the process of searching databases to find new information through combining existing data and/or making predictions about future behaviors based on data patterns.[41] According to Solove and Hoofnagle "[i]ncreasingly, such data analysis is being outsourced to database companies."[42] Although Congress withdrew funding from TIA in 2003, new government data mining operations that perform the same functions have emerged.[43] Such new data mining operations include fusion centers.

ii. Fusion Centers

Fusion centers have been described as "an amalgamation of commercial and public sector resources for the purpose of optimizing the collection, analysis, and sharing of information on individuals."[44] Fusion centers are collecting and analyzing data from "banking and finance, real estate, education, retail sales, social services, transportation, postal and shipping, and hospitality and lodging transactions."[45] Surveying government data mining operations, fusion centers may be "just the tip of the iceberg."[46] According to Christopher Slobogin, "just one year after TIA's demise, 52 federal agencies were using or were planning to use data mining, for a total of 199 data mining efforts, 68 planned and 131 operational. Of these programs, at least 122 are designed to access 'personal' data."[47]

In light of the fact that regulations on commercial data brokers are lax, and the government can obtain any information these institutions collect, the government enjoys all but unlimited access to individuals' modern papers and effects. Under the Fourth Amendment, a government search of individuals' papers and effects is only reasonable when supported by a proper warrant.[48] By leveraging the services of commercial data brokers, however, the government is

---

[38] DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 175 (2004).
[39] Andrew E. Taslitz & James Coleman, *The Death of Probable Cause*, *in* 107 Law and Contemporary Problems, 121 (2010).
[40] *Id*.
[41] *Id* at 41.
[42] Solove & Hoofnagle, *supra* note 22, at 364.
[43] *Id*.
[44] Lillie Coney, *Statement to the Department of Homeland Security Data Privacy and Integrity Advisory Committee*, Electronic Privacy Information Center, 1 (Sept 19, 2007), http://www.epic.org/privacy/fusion/fusion-dhs.pdf.
[45] Christopher Slobogin, *Government Data Mining and the Fourth Amendment,* 75 U. Chi. L. Rev. 317, 318 (2008).
[46] *Id.* at 319 (commenting on government Information Fusion Centers).
[47] *Id*.
[48] U.S. Const. amend. IV ("The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.").

effectively searching individuals' papers and effects without providing any justification.[49] This regime is paradoxical as it provides for government searches that appear fundamentally inconsistent with the Fourth Amendment.

C. Business Applications

In his book *No Place to Hide*, Robert O'Harrow takes a particular interest in ChoicePoint, a former commercial data broker that was purchased by LexisNexis' parent company Reed Elsevier in 2008.[50] Today, LexisNexis is one of the database industry's "larger data brokers."[51] O'Harrow cites the case of Mary Boris as an example of the ongoing problems with commercial database business applications. [FN52] For more than two years, Boris tried to work with ChoicePoint to correct inaccurate home insurance claims reported in the company's Comprehensive Loss Underwriting Exchange—commonly known as CLUE.[53] "[Boris] discovered she was no longer covered when an insurance representative said that her record was sullied by four claims for fire damage and one theft. She checked with other insurers and their story was the same."[54] "Using almost 200 million records, contributed by all major insurance companies, CLUE creates a 'score' on virtually every policy holder in the country."[55]

Although the Fair Credit Reporting Act requires private enterprise to maintain accurate records and be responsive to consumers, Boris was neglected by ChoicePoint when she contacted the company in hopes of remedying the false information. Boris eventually brought suit against ChoicePoint under the FCRA and was awarded more than $400,000 in damages.[56]

III. EMPLOYER APPLICATIONS

Employer access to perpetual criminal records has created problems for some hopeful employees. "In 41 states, people accused or convicted of crimes have the legal right to rewrite history. They can have their criminal records expunged, and in theory that means that all traces of their encounters with the justice system will disappear."[57] The problem of perpetual criminal records arises from commercial data brokers' maintenance of criminal records. Criminal records that have been expunged from public databases are regularly appearing in background checks ordered by employers.[58] In 2006, the New York Times reported how this happened to a man named Mr. Guevares.[59]

---

[49] *See* Taslitz & Coleman, *supra* note 39, at 122 (noting that the "use of computers to aggregate personal information . . . can proceed without having to check with a magistrate or provide any justification for doing so.").
[50] O'Harrow, *supra* note 32, at 140.
[51] Solove and Hoofnagle, *supra* note 22, at 363.
[52] O'Harrow, *supra* note 32, at 140.
[53] *Id*.
[54] *Id*. at 139.
[55] *Id*. at 140.
[56] *Id*.
[57] Adam Liptak, *Expunged Criminal Records Live to Tell Tales*, N.Y. Times October 17, 2006, http://www.nytimes.com/2006/10/17/us/17expunge.html (last visited Oct. 7, 2011).
[58] *Id*.
[59] *Id*.

Mr. Guevares' story involves Acxiom, another one of the database industry's "larger data brokers."[60] Acxiom is a billion-dollar commercial data broker that possesses personal information on most adults in the United States.[61] Acxiom provided Tyco Healthcare Group with a report on Guevares who had been extended an offer of employment by the latter. "Tyco promptly withdrew the offer . . . on its mistaken understanding that he had committed a misdemeanor and had lied on his application about whether he had ever been 'convicted of any crime which was not expunged or sealed by a court.'"[62] Guevares eventually received a "substantial settlement," and Acxiom agreed to train employees not to report "non-criminal conviction information."[63]

Another employer database application is ChoicePoint's "Esteem" operation.[64] O'Harrow describes Esteem as "a sort of blacklist of people who have been accused or convicted of shoplifting. Dozens of retailers now contribute reports to the system, in turn using it to block the hiring of people included there."[65] This appears highly problematic as a mere accusation under such a framework may preclude individuals from securing work in an industry for which they are otherwise qualified.

IV. AREAS OF PRIVACY LAW

Privacy law has been criticized as suffering from an "inability to conceptualize itself."[66] "The real challenge for scholarship falling in this category going forward will be to bring some coherence to the field. Whether that coherence can best be obtained within the rubric of 'privacy' or some other term or terms will remain to be seen."[67] Richards suggests that current information privacy efforts would be more effective if they abandoned the term "privacy" for "'confidentiality,' 'data protection,' or some new term altogether" as privacy is an inherently nebulous term.[68] Nonetheless, authorities have identified three distinct types of privacy.

A. Informational Privacy

This note focuses upon privacy problems involving individuals' personal information (e.g., the decentralization and aggregation of personal information and the commercial data broker paradox). Solove has identified problems of diminished control over personal information as problems of "informational privacy."[69]

---

[60] Solove and Hoofnagle, *supra* note 22,22 at 363.
[61] O'Harrow, *supra* note 32, at 34.
[62] Liptak, *supra* note 57, at 1.
[63] *See* Legal Action Center publication on Criminal Record Based Discrimination citing *Guevares v. Acxiom*, 06-CV-2930, E.D.N.Y. (2006) http://www.lac.org/doc_library/lac/publications/leading_cases.pdf, (last visited on Oct. 7, 2011)
[64] O'Harrow, *supra* note 32, at 132.
[65] *Id*.
[66] Richards, *supra* note 2 at 1140.
[67] *Id*.
[68] *Id*. at 1094.
[69] Daniel J. Solove, *Identity Theft, Privacy, and the Architecture of Vulnerability*, 54 Hastings L.J. 1227, 1228 (2003).

Informational privacy problems -- such as government data mining dragnets of commercial databases—have given rise to negligible litigation.[70] The lack of informational privacy litigation is often attributed to the fact that the Supreme Court has held that "government efforts to obtain personal information 'voluntarily' surrendered to third parties such as banks, phone companies, and accounting firms" do not implicate the Fourth Amendment.[71] According to the Court, individuals assume the risk of disclosure of personal information by dealing with such services, and lack standing to bring a Fourth Amendment challenge.[72]

B. Spatial Privacy

While informational privacy injuries typically stem from a loss of control over personal information, spatial privacy injuries stem from a violation of personal space. Legal authorities have identified both informational and spatial privacy problems with the networked computer.[73] Today's networked computer serves as a center of directing everything from one's social life to financial matters. The networked computer tends to centralize functions that—no more than a decade ago—would have required significant space in the home (e.g., an appropriate setting to meet with friends and share pictures and information and large disc drives or file cabinets for storing information). The networked computer appears to be assuming roles once monopolized by the living room and home office (e.g., a meeting place that facilitates interaction, directing workflow, and storing documents).

C. Decisional Privacy

Another area of privacy is "decisional privacy."[74] "Decisional privacy is usually defined as the right of individuals to make certain kinds of fundamental choices with respect to their personal and reproductive autonomy, and has its locus in the constitutional jurisprudence of *Roe v. Wade* and *Griswold v. Connecticut*."[75] Solove and several other legal authorities see informational privacy as largely unrelated to decisional privacy.[76] Richards, however, has argued "the informational/decisional binary is at best a fuzzy means of categorizing two quite related interests . . .". [77] He has proposed that the First Amendment privacy protections provided in *Griswold* may apply to informational privacy problems involving the government as the case is "concerned with government access to information."[78] Although it is possible that decisional privacy cases could eventually be read to protect information privacy rights, privacy law

---

[70] Taslitz and Coleman, *supra* note 39, at 121.
[71] *Id.* at 121-122.
[72] *Id.* at 122.
[73] *See* Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1202 (1998) (describing "spatial privacy").
[74] Richards, *supra* note 2, at 1087.
[75] *Id.* at 1089.
[76] *Id*. at 1105.
[77] *Id*. at 1093.
[78] Richards, *supra* note 2, at 1107.

authorities appear to be directing their efforts toward legislative solutions to federal privacy legislation.[79]

V. CURRENT U.S. PRIVACY PROTECTIONS

This section will assess current U.S. privacy protections by reviewing federal privacy legislation and privacy torts. The historic battle between privacy and technology is a touchstone of this note's analysis. Although this battle has been underway for no less than a century,[80] technological affronts to privacy appear to be growing in number and intensity in the electronic age. The growing body of federal privacy legislation over the past 40 years attests to this.

A. Federal Privacy Legislation

Although most industrialized nations have comprehensive data protection laws, the United States has maintained a sectored approach where certain industries are covered and others are not.[81] This fragmented approach is reflected across federal privacy legislation including the Privacy Act, the Fair Credit Reporting Act, and the Electronic Communications Privacy Act.

i. Privacy Act of 1974 ("Privacy Act")

In 1973, a report titled *Computers and the Rights of Citizens* was issued to the U.S. Secretary of Health, Education, and Welfare.[82] Among legal authorities, this report is commonly referred to as the HEW report. Today, the HEW report is as salient as ever. "Even in non-governmental settings, an individual's control over the personal information that he gives to an organization, or that an organization obtains about him, is lessening as the relationship between the giver and the receiver of personal data grows more attenuated, impersonal, and diffused."[83] It was in response to this report that Congress enacted the Privacy Act. [84] The Privacy Act mandated a set of Fair Information Principles including the following guidelines:

(a) there must be no personal data record-keeping system whose very existence is secret; (b) there must be a way for an individual to find out what information about him is in a record and how it is used; (c) there must be a way for an individual to prevent information about him that was obtained for one purpose from being used or made available for other purposes without his consent; (d) there must be a way for an individual to correct or amend a record of identifiable information about him; and (e) any organization creating, maintaining, using, or disseminating

---

[79] *See* Solove and Hoofnagle, *supra* note 22, at 357 (commenting upon their model regime can be incorporated into privacy regulation in the United States).
[80] *See* Warren and Brandeis, *supra* note 10, at 193.
[81] *See* Solove and Hoofnagle, *supra* note 22, at 357.
[82] *See* OFFICE OF THE ASSISTANT SEC'Y FOR PLANNING AND EVALUATION, U.S. DEP'T OF HEALTH AND HUMAN SERV., RECORDS, COMPUTERS AND THE RIGHTS OF CITIZENS: REPORT OF THE SECRETARY'S ADVISORY COMMITTEE ON AUTOMATED PERSONAL DATA SYSTEMS (1973).
[83] *Id.* at 9.
[84] Zittrain, *supra* note 4, at 201-202 (commenting on how controversy over President Nixon's use of government records and the HEW report generated political momentum for Congress to enact the Privacy Act).

records of identifiable personal data must assure the reliability of the data for their intended use and must take precaution to prevent misuse of the data.[85]

These principles continue to inform emerging notions of privacy law.[86] Although the original draft of the Privacy Act applied to both public and private databases, the final version of the act applied only to the government.[87] This gap provided for the inevitable rise of commercial data brokers.

ii. Freedom of Information Act ("FOIA")

FOIA provides for the full or redacted release of previously unreleased information controlled by the U.S. government. "If you have ever applied for a federal benefit or received a student loan guaranteed by the government, you are probably the subject of a file. There are records on every individual who has ever paid income taxes or received a check from Social Security or Medicare."[88] The Privacy Act amended FOIA to guarantee individuals three primary rights:

(1) the right to see records about oneself, subject to the Privacy Act's exemptions; (2) the right to amend a nonexempt record if it is inaccurate, irrelevant, untimely, or incomplete; and (3) the right to sue the government for violations of the statute, such as permitting unauthorized individuals to read your records.[89]

iii. Fair Credit Reporting Act ("FCRA")

The FCRA requires that consumer credit reporting agencies maintain "reasonable procedures for meeting the needs of commerce for consumer credit, personnel, insurance, and other information in a manner which is fair and equitable to the consumer, with regard to the confidentiality, accuracy, relevancy, and proper utilization of such information."[90] The FCRA requires credit reporting agencies to maintain procedures to ensure "maximum possible accuracy."[91] Solove and Hoofnagle note that "nowhere in the statute does it authorize companies to charge a fee for such service."[92] "[C]redit card companies have architected the current credit system that has put consumers at risk, and then turned this risk into a business opportunity to market credit monitoring."[93]

---

85 *See* OFFICE OF THE ASSISTANT SEC'Y FOR PLANNING AND EVALUATION, U.S. DEP'T OF HEALTH AND HUMAN SERV., RECORDS, COMPUTERS AND THE RIGHTS OF CITIZENS: REPORT OF THE SECRETARY'S ADVISORY COMMITTEE ON AUTOMATED PERSONAL DATA SYSTEMS (1973).

86 *See* Ludington, *supra* note 30, at 180 (advocating "a minimum standard of care on private entities to abide by the same standards . . . that bind the federal government").

87 *Id.*

88 *See* the U.S. Department of Justice's explanation of information collected on individuals and the Privacy Act's amendments to FOIA (available at http://www.foia.gov/federal-records.html).

89 *Id.*

90 *Sloane v. Equifax*, 510 F.3d 495 (4th Cir. 2007), (the 4th Circuit applying the FCRA Pub. L. No. 91-508, 84 Stat. 1114 (codified as amended at 15 U.S.C. §§1681-1681x)).

91 Solove & Hoofnagle, *supra* note 22, at 393.

92 *Id.*

93 *Id.*

The FCRA provides a private cause of action for individuals injured by violations of its provisions. Plaintiffs can recover both actual and punitive damages for willful violations of the statute. Plaintiffs can also recover actual damages for negligent violations. "Actual damages may include not only economic damages, but also damages for humiliation and mental distress. The statute also provides that a successful plaintiff suing under the FCRA may recover reasonable attorney's fees."[94]

1. Fair and Accurate Credit Transactions Act of 2003 ("FACTA")

FACTA was passed in 2003 as an amendment to the FCRA.[95] FACTA has provided free annual credit reports to all consumers, enacted additional safeguards in the credit reporting system to prevent such fraud, and has provided the victims of identity theft with additional tools to help them restore their credit record. [96]

2. Gaps in the FCRA

Although the FCRA provides individuals with several measures of protection, these provisions are not without shortcomings. Recent amendments to the FCRA have precluded states from enacting legislation that would offer more comprehensive privacy protections.[97] Ironically, several of the FCRA's most significant protections originated in the states (e.g., most FACTA reforms were first passed in the states).[98] This irony highlights the fact that the FCRA is preempting the innovative role of the states to "serve as a laboratory; and try novel social and economic experiments without risk to the rest of the country."[99]

Another gap in the FCRA is its failure to provide individuals with visibility to the quantum of their information that has been released and to whom. This gap fails to protect one from "downstream sale of his nonfinancial personal information."[100] Examples of downstream uses include secondary uses (e.g., Bank of America pulling a report on an individual, storing the information, and later selling or sharing it with another entity).

"To the extent that a data trader functions as a consumer reporting agency (CRA), it will fall within the limitations of the Fair Credit Reporting Act."[101] Commercial data brokers, however, are not subject to the limitations of the FCRA, as they are not considered credit reporting agencies.[102] Although the FCRA defines credit reporting agencies as "entities that assemble and sell credit or other information about individuals," commercial data brokers do not fall under this

---

[94] See 15 U.S.C. §§1681 n(a)(3)-o(a)(2).
[95] *See* the Fair and Accurate Credit Transactions Act (FACTA) of 2003, Pub. L. No. 108-159, 117 Stat. 1952 (codified as amended across sections of 15 U.S.C.) (amending the Fair Credit Reporting Act of 1970).
[96] *See* DEE PRIDGEN & RICHARD M. ALDERMAN, CONSUMER CREDIT AND THE LAW, (Clark Boardman Callaghan (September 2, 2010).
[97] Solove & Hoofnagle, *supra* note 22, at 380.
[98] *Id*. at 381, 402.
[99] New State Ice Co. v. Liebmann, 285 U.S. 262, 311 (1932) (Brandeis, J., dissenting).
[100] *See* Ludington, *supra* note 30, at 158 (commenting on failed state and federal legislative efforts to provide remedies to individuals injured by unfair or insecure data practices).
[101] *Id*. at 174.
[102] *Id*.

classification.[103] The FBI has offered its reasoning why commercial data brokers are not subject to the FCRA:

In this instance, none of the information that the FBI would seek to review has been collected by ChoicePoint for any of the [FCRA] purposes. … Because ChoicePoint does not collect 'public record information' for any of the highlighted purposes [under the FCRA], ChoicePoint is not acting as a 'consumer reporting agency' for the purposes of the FCRA, and the collected information therefore does not constitute a 'consumer report.'[104]

iv. Electronic Communications Privacy Act ("ECPA")

In 1986, Congress enacted the Electronic Communications Privacy Act ("ECPA"). The ECPA includes three acts: the Wiretap Act (which updated Title III of the Omnibus Crime Control and Safe Streets Act of 1968), the Stored Communications Act, and the Pen Register Act.[105] "[I]t is important to know that the ECPA classifies all communications into three types: (1) 'wire communications'; (2) 'oral communications'; and (3) 'electronic communications.' Each type of communication is protected differently. As a general matter, wire communications receive the most protection and electronic communications receive the least." [106]

A "wire communication" is defined in 18 U.S.C. §2510(1). "Wire communication" involves all "aural transfers" that travel through a wire or a similar medium.[107] Under §2510(2), an "oral communication" is defined as a communication "uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation."[108] Intercepted oral communications covered by this legislation are typically intercepted by audio recording and transmission devices.[109]

Under 18 U.S.C. § 2510(12), the definition of "electronic communication" is provided as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectric, or photooptical system that affects interstate or foreign commerce . . . ."[110] This definition appears to apply to most transmissions that take place across networked computers (e.g., emails, text messages, data downloading and uploading). Once these communications become classified as "electronic storage," however, they come under the protections of the second act of the ECPA, the Stored Communications Act ("SCA").[111]

The SCA states that it is a criminal offense when one "(1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or (2) intentionally exceeds an authorization to access that facility . . ."[112] If the government seeks access to a communication that has been in electronic storage for less than 180 days it must

---

[103] *Id*.
[104] Solove & Hoofnagle, *supra* note 22, at 365.
[105] SOLOVE & ROTENBERG, INFORMATIONAL PRIVACY LAW 264-65 (Aspen Publishers 1974) (2005).
[106] *Id*. at 266.
[107] 18 U.S.C. § 2510(1) (West, Westlaw through P.L. 112-28 approved 8-12-11).
[108] 18 U.S.C. § 2510(2).
[109] SOLOVE & ROTENBERG, *supra* note 105, at 266.
[110] 18 U.S.C. § 2510(12).
[111] SOLOVE & ROTENBERG, *supra* note 105, at 270.
[112] 18 U.S.C. § 2701(a).

produce a warrant. As with any warrant for the seizure of papers and effects, the government must satisfy a standard of probable cause.[113] If the communication has been in storage for more than 180 days, however, the government need merely: 1) provide prior notice to the subscriber; and 2) produce a court order supported by "specific and articulable facts showing that there are reasonable grounds" that the communication is relevant to a criminal investigation.[114]

v. Gramm-Leach-Bliley Act ("GLBA")

The GLBA (also known as the Financial Services Modernization Act of 1999) "allowed for the creation of giant financial supermarkets that could own investment banks, commercial banks and insurance firms, something banned since the Great Depression. Its passage, critics say, cleared the way for companies that were too big and intertwined to fail."[115] Seemingly recognizing the inevitable size and power of the financial supermarkets for which it was paving the way, the GLBA codified rules such as the Financial Privacy and Safeguard Rules.[116]

The GLBA's Financial Privacy Rule provides that financial institutions must provide each of their customers with an annual privacy notice detailing their rights to opt out of various uses of their personal information.[117] The privacy notice must also provide consumers with an explanation of the information collected about them and how such information is used, shared, and protected.[118]

The GLBA's Safeguard Rule provides that financial institutions must develop a written information security plan to protect consumers' "nonpublic personal information."[119] Under the GLBA, financial institutions cannot share consumers' nonpublic personal information with non-affiliated entities without giving the consumer the right to "opt out."[120]

Enforcement of the GLBA is assigned to federal agencies (e.g., the FTC).[121] Although there is no private right of action under the GLBA, and privacy notices are often confusing for consumers, this legislation has proven valuable by providing a roadmap for privacy practices and compliance for the financial service industry.

B. Privacy Torts

In looking to who fired the first shot in battle between privacy and technology, one might argue it was the late nineteenth century press and its modern devices.[122] Indeed, Warren and Brandeis' article directly addressed this threat and spun a series of torts with their locus in

---

[113] *See* 18 U.S.C. § 2703(a).
[114] *Id*. § 2703(b)(B)(ii), (d).
[115] Damien Paletta & Kara Scannell, *Ten Questions for Those Fixing the Financial Mess*, WALL ST. J., Mar. 10, 2009, http://online.wsj.com/article/SB123665023774979341.html.
[116] *See* 15 U.S.C. § 6803 (Financial Privacy Rule), *and* 15 U.S.C. § 6805 (Safeguard Rule).
[117] 15 U.S.C. § 6802(b).
[118] *Id*. § 6803(a), (c).
[119] *Id*. § 6803(c)(3).
[120] *Id*. § 6802(b).
[121] *Id.* § 6805(a).
[122] *See* Warren & Brandeis, *supra* note 10, at 197 (arguing the law affords a principle to protect the privacy of the individual from invasion by the modern device).

privacy. These torts include intrusion upon seclusion, defamation, false light, and publicity to private life.[123]

US citizens do not enjoy any fundamental protections against unreasonable searches and seizures by non-state actors. Consequently, private enterprise can often unreasonably violate one's Fourth Amendment papers and effects without violating any criminal code or regulation. There are several civil remedies, however, that individuals may advance when they feel their privacy has been violated.

In the context of data privacy harms, the requisite elements of these torts are difficult to satisfy, and the injuries can be difficult to demonstrate. As aptly described by Solove and Hoofnagle, "[t]he problem with applying common-law torts is that data privacy harms are often ill-defined and under-developed in the common law."[124]

i. Intrusion Upon Seclusion

Intrusion upon seclusion often involves sensory intrusions such as eavesdropping and wiretapping, but has also been held to apply to specific uses of individuals' personal information.[125] The Restatement (Second) of Torts §652B provides: "One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person."[126] The court has interpreted this action as having two elements: (1) intrusion into a private place, conversation or matter, (2) in a manner highly offensive to a reasonable person.[127]

In order to advance a successful intrusion upon seclusion claim, one must show both an objective and subjective expectation of privacy. The expectation of privacy must have been objectively reasonable and the injured party must have actually expected privacy.[128] As demonstrated in *Dwyer v. American Express Co.*, successfully showing an intrusion often proves very difficult when individuals have consented—willingly or otherwise—to the dissemination of their personal information in exchange for a service.[129] In *Dwyer*, the court held "a cardholder is voluntarily, and necessarily, giving information to defendants that, if analyzed, will reveal a cardholder's spending habits and shopping preferences. We cannot hold that a defendant has committed an unauthorized intrusion by compiling the information voluntarily given to it and then renting its compilation."[130]

---

[123] *See Id.* at 193–95 (noting "numerous mechanical devices threaten to make good the prediction that 'what is whispered in the closet shall be proclaimed from the house-tops.'").
[124] Solove & Hoofnagle, *supra* note 22, at 386.
[125] *See Shulman v. Group W Prod., Inc.*, 955 P.2d 469 (Cal., 1998) (citing the application of intrusion upon seclusion to matters involving eavesdropping and wiretapping); *See Weld v. CVS Pharmacy, Inc.*, 10 Mass. L. Rptr. 217, 1999 WL 494114, at *1 (Mass. Supp., 1999) (applying intrusion upon seclusion to the defendant's aggregation of name, address, and medical prescription data for direct marketing purposes).
[126] RESTATEMENT (SECOND) OF TORTS § 652B.
[127] *See Shulman*, 955 P.2d at 490-492 (reviewing the plaintiff's expectations of privacy in a rescue helicopter covered by a news agency).
[128] *Id.*
[129] *See* Dwyer v. American Express Co., 652 N.E.2d 1351, 1354 (Ill. App. Ct. 1995).
[130] *Id.*

In *Weld v. CVS Pharmacy, Inc.*, however, the court held that the compilation of name and address data with medical prescription records invaded the plaintiff's privacy.[131] In *Weld*, the defendant mailed the plaintiff materials targeted to their specific medical condition as a part of a direct marketing campaign.[132] The court's analysis upon how the plaintiff's personal information was used and not how the defendant obtained it appears to hold promise for the application of the tort of intrusion to problems of personal information aggregation.

ii. Defamation

The tort of defamation varies from the torts of intrusion upon seclusion and publicity to private life as a defamatory statement must be false. A true statement that harms the reputation of another cannot give rise to liability for defamation. The Restatement (Second) of Torts §559 provides that a defamatory statement "tends to harm the reputation of another or lower him in the estimation of the community or to deter third persons from associating or dealing with him."[133] Defamation is differentiated into two torts, libel and slander. Libel consists of written statements, whereas slander is spoken.

iii. False Light

The tort of false light provides a remedy against anyone who publicizes a matter concerning the plaintiff that is both false and objectionable. The Restatement (Second) of Torts § 652E provides:

> One who gives publicity to a matter concerning another that places the other before the public in a false light is subject to liability to the other for invasion of his privacy, if (a) the false light in which the other was placed would be highly offensive to a reasonable person, and (b) the actor had knowledge of or acted in reckless disregard as to the falsity of the publicized matter and the false light in which the other would be placed.[134]

Although both false light and defamation attach liability for material false statements, false light can compensate exclusively for emotional distress whereas defamation requires reputational injuries. As in the case of Mary Boris, the tort of false light can make one whole, but the process is often arduous. Pursuing redress is a time consuming process, and injuries quickly amass.

iv. Publicity to Private Life

The tort of Publicity to Private Life highlights the gap in current tort law as it pertains to emerging privacy problems. The Restatement (Second) of Torts § 652D provides:

---

[131] *See Weld*, 10 Mass. L. Rptr. 217, 1999 WL 494114 (Mass. Super. Ct., 1999) at *1.
[132] *Id.*
[133] *See* THE RESTATEMENT (SECOND) OF TORTS §559 (1977).
[134] *See* THE RESTATEMENT (SECOND) OF TORTS § 652E (1977).

> One who gives publicity to a matter concerning the private life of another is subject to liability to the other for invasion of his privacy, if the matter publicized is of a kind that (a) would be highly offensive to a reasonable person, and (b) is not of legitimate concern to the public.[135]

Like intrusion upon seclusion, in order to successfully assert publicity to private life one must satisfy both elements.

Long held conceptions of "the public eye" highlight the inadequacy of the tort of publicity to private life to address modern threats to privacy. In *Sipple v. Chronicle*, Oliver Sipple failed to establish a publicity to private life claim as the court found that the information published was not private.[136] In 1975, Sipple intervened in an assassination attempt against President Ford—quite possibly saving the President's life. It quickly became national news that Sipple not only saved the President's life, but that Sipple was also gay.

Sipple filed action against the Chronicle Publishing Company, the Los Angeles Times, and numerous other newspapers. He claimed that "said publications were highly offensive to [him] inasmuch as his parents, brothers and sisters learned for the first time of his homosexual orientation; and that as a consequence . . . was abandoned by his family, exposed to contempt and ridicule causing him great mental anguish, embarrassment and humiliation."[137]

On appeal in 1984, the court held "there is no liability . . . when the further publicity relates to matters which the plaintiff leaves open to the public eye" citing the fact that Sipple frequented well-known gay sections of San Francisco.[138] This logic from *Sipple* is troubling as it flows to most circumstances of most individuals' lives (e.g., individuals may not wish to have the fact published that they see certain medical specialists, frequent particular stores, etc.).

Tying this example to the wares of the information age, today's multifunctionality of networked computers perpetually places individuals in the public eye. Every individual is a potential media agent, as most smartphones and mobile devices tout camera and video recording functionality. With the touch of a button, many of these devices can publish pictures and video to widely viewed internet locations such as Facebook and YouTube. The next section addresses this, and other emerging privacy problems—problems of "Privacy 2.0."

VI. THE RISKS OF GENERATIVITY: PRIVACY 2.0

The term "Privacy 2.0" was coined by Johnathan Zittrain, who is both a Professor of Law at Harvard Law School and a Professor of Computer Science at Harvard's School of Engineering and Applied Sciences.[139] In his book, *The Future of the Internet and How to Stop It*, Zittrain paints a sobering picture of the future of privacy in the United States. "Indeed, the Net enables individuals in many cases to compromise privacy more thoroughly than the government and commercial institutions traditionally targeted for scrutiny and regulation. The standard

---

[135] *See* THE RESTATEMENT (SECOND) OF TORTS § 652D (1977).
[136] Sipple v. Chronicle, 201 Cal. Reptr. 665 (Cal. App. 1 Dist., 1984).
[137] *Id.*
[138] *Id.*
[139] Zittrain, *supra* note 4, at 200.

approaches that have been developed to analyze and limit institutional actors do not work well for this new breed of problem…"[140]

The FCRA and Privacy Act are examples of standard approaches taken to limit institutional actors. "The FCRA and Privacy Act have thus provided a basic framework of privacy protection, with the FCRA addressing the key private sector uses of personal data and the Privacy Act addressing public sector uses."[141] Zittrain casts these responses as answers to "Privacy 1.0" problems.[142]

Many of Zittrain's insights pertain to the principle of generativity. Generativity is the ability of a self-contained system to provide an independent ability to create, generate, or produce content without any input from the originators of the system (e.g., individuals using smartphones to record videos of anything they want to—along with their remarks—and publishing the video instantly to the internet). Zittrain remarks that "emerging threats to privacy serve as an example of generativity's downsides on the social layer, where contributions from remote amateurs can enable vulnerability and abuse that calls for intervention."[143] Zittrain and other authorities propose methods of intervention that are central components of model solutions.

VII. MODEL SOLUTION

The privacy of people in the United States is being challenged by the government, private enterprise, and individuals. Etzioni calls for a higher standard for when and how privacy should be violated stating: "[W]hat is called for are not some limited, ad-hoc concessions to the common good, extended if and when a specific and strong case can be presented that privacy must be curbed. What is required is a fundamental change in civic culture, policymaking, and legal doctrines."[144]

A. Government Solutions

Solove and Hoofnagle suggest that the government's interactions with individuals' personal information be reined in by an updated Privacy Act.[145] Over thirty years have passed without a major reexamination of the Privacy Act. "There must be a meaningful regulation that limits the collection of personal data, lists acceptable uses, guarantees accuracy, provides security, and restricts retention of personal information by government agencies, especially since they are acquiring more and more data about individuals."[146]

---

[140] *Id*. at 200-01.
[141] Solove & Hoofnagle, *supra* note 22, at 361-62.
[142] Zittrain, *supra* note 4, at 201-02.
[143] *Id.* at 205.
[144] Etzioni, *supra* note 24, at 3-4.
[145] Solove & Hoofnagle, *supra* note 22, at 380.
[146] *Id*.

B. Private Enterprise Solutions

The current scheme of self-regulation enjoyed by commercial data brokers and large segments of private enterprise is fundamentally flawed. These entities have a diminishing motive to refrain from collecting, storing, and using more of individuals' personal information as these pursuits grow more profitable. As noted by Acxiom, "[d]eep consumer insights in the form of Acxiom's data enhancements, lists, demographics, segmentation and buying behavior enable effective and profitable marketing initiatives and business decisions."[147]

Sarah Ludington has argued that greater misuses of individuals' personal information will inevitably arise alongside legitimate innovations in data technology.[148] She contends that federal legislation is "the most effective way to rein in the data traders."[149] Many commercial data brokers and their customers can ill afford to unilaterally change their practices of using individuals' personal information. Across sectors, entities compete against one another by using individuals' personal information to meet goals (and, in the case of the private sector, generate profitability). Under an updated Privacy Act, data traders and their customers could align their practices with defined limitations without suffering against their competition. According to Ludington, "a patchwork of common law tort regimes may have data traders begging for comprehensive federal legislation."[150]

With respect to the vulnerability of the credit card system and the problematic nature of the credit card industry selling consumers a fix to a problem they created—Solove and Hoofnagle propose a fix of their own.[151] These authorities argue that "under their FCRA duty to maintain the maximum possible accuracy, consumer reporting agencies should provide free credit monitoring to individuals."[152]

Addressing the problem of perpetual criminal records in employment, a solution can be modeled on current state codes that put the burden on accuracy of information on employers. "Illinois, for instance, prohibits prospective employers from asking about or making decisions based on expunged or sealed criminal histories."[153] A common theme emerges across model measures—limitations that focus upon how personal information is being used (and not upon whom or what is using it) appear to hold the most promise for protecting individuals' privacy.

C. Civil Remedy Solutions

As analyzed above, the application of current common law torts to emerging data privacy problems is often problematic. Ludington has contended that a new tort for the misuse of personal information could prove the solution.[154] She argues that the creation of a new civil

---

[147] *See* Acxiom commenting on their consumer insight products at Axiom.com (http://www.acxiom.com/Ideas-and-Innovation/Self-Assessment-Tools/).
[148] *See* Ludington, *supra* note 30, at 189.
[149] *Id*.
[150] *Id*.
[151] Solove& Hoofnagle, *supra* note 22, at 393.
[152] *Id*.
[153] Adam Liptak, *Expunged Criminal Records Live to Tell Tales*, THE NEW YORK TIMES (Oct. 17, 2006) http://www.nytimes.com/2006/10/17/us/17expunge.html.
[154] Ludington, *supra* note 30, at 142.

remedy that would impose a minimum standard of care on private entities to abide by the Fair Information Principles holds promise.[155] By applying the robust protections of the HEW report's Fair Information Principles, such a tort would undoubtedly address a number of emerging privacy issues.

D. Privacy 2.0 Solutions

With respect to problems of Privacy 2.0, solutions can be introduced from the same source from which the problem has arisen—individuals' generativity. According to Zittrain:

Enduring solutions to the new generation of privacy problems brought about by the generative Internet will have as their touchstone tools of connection and accountability among the people who produce, transform, and consume personal information and expression: tools to bring about social systems to match the power of the technical one.[156]

As more people utilize internet social systems, the prospects of keeping Privacy 2.0 problems in check grow (e.g., a Facebook group of like-minded people built around criticism of individuals who violate the privacy of other individuals garnering attention and influencing behaviors).

CONCLUSION

Despite the government's efforts to balance intrusions, it remains the single entity the people of the United States most fear will compromise their privacy.[157] Although the networked computer appears to be pushing "our own walls" outward, the people of the U.S. are not receiving more privacy protections.[158] Alternatively, it appears our own walls are being traversed more via government searches made possible by commercial data brokers. A prevalent scheme of self-regulation allows commercial data brokers liberties with individuals' personal information that even the government does not enjoy. Paradoxically, the government is not limited from obtaining individuals' personal information using these commercial data brokers, personal information the government would otherwise be without. Significant gaps in a patchwork of dated legislation are allowing the government all but unlimited access to personal information on individuals in the information age. This troubling development is not consistent with the plain language, context, or spirit of the Fourth Amendment.

---

[155] *Id.* at 180.
[156] Zittrain, *supra* note 4, at 234.
[157] *See* Etzioni, *supra* note 24, at 9-10 (citing the government as "the villain that champions of privacy traditionally fear the most").
[158] *See* Whitman, *supra* note 3, at 1151 (describing the American conception of privacy).