THE GEORGE WASHINGTON UNIVERSITY LAW SCHOOL
PUBLIC LAW AND LEGAL THEORY WORKING PAPER NO. 102

THE NEW VULNERABILITY: DATA SECURITY AND PERSONAL INFORMATION

Daniel J. Solove

Accepted Paper

Book chapter for forthcoming book

published by Stanford University Press

THE NEW VULNERABILITY: DATA SECURITY AND PERSONAL INFORMATION

by Daniel J. Solove[1]

Data security is quickly becoming one of the major concerns of the Information Age. Computer networks are vulnerable to siege from hackers, viruses, intercepted communications, and electronic surveillance.[2] Much of the data residing in these computer networks pertains to our personal lives. Increasingly, extensive digital dossiers about us are being constructed as businesses and the government gather pieces of personal data and assemble them together in databases. Hundreds—perhaps thousands—of entities may have our personal information.[3] Our dossiers play a profound role in our lives. They are used to assess our reputation and credibility. They are examined to determine whether we receive a loan, a job, a license—and even whether we are detained or arrested by the police. Because so many critical decisions are based on our dossiers, ensuring that they are accurate and protected from tampering is of paramount importance.

Unfortunately, our dossiers are virtually unguarded. Anybody can readily tap into our dossiers – and they do. Identity theft—the use of personal information to illegally access existing financial accounts, open fraudulent accounts, or obtain credit cards in other people's names—is the most rapidly growing type of white-collar criminal activity.[4] Complaints of identity theft in the United States rose a staggering 88% from 2001 to 2002.[5] According to a Federal Trade Commission (FTC) estimate in September 2003, "almost 10 million Americans have discovered that they were the victim of some form of ID Theft within the past year."[6] Collectively, victims labored for almost 300 million hours to resolve the tribulations caused by identity theft.[7] The FTC estimates that consumers lost $5 billion due to identity theft and other information abuses.[8]

Although abuses of personal information are becoming ubiquitous in the digital age, not enough thought has been given to how the law should

---

[1] Associate Professor, George Washington University Law School; J.D. Yale. I would like to thank Jake Barnes for his help in the tort law discussions of this Essay. To the extent my knowledge of tort law is accurate, I accept full responsibility. As for the errors, blame Jake. Chris Hoofnagle, Ted Janger, and Paul Schwartz provided helpful comments on the manuscript.

[2] For an extensive account of security threats to computer networks, see BRUCE SCHNEIER, SECRETS AND LIES: DIGITAL SECURITY IN A NETWORKED WORLD (2000).

[3] Daniel J. Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy,* 53 Stan. L. Rev. 1393, 1403-13 (2001).

[4] *See* Jennifer 8. Lee, *Fighting Back When Someone Steals Your Name*, N.Y. Times, April 8, 2001; *see also* Jennifer 8. Lee, *Identity Theft Victimizes Millions, Costs Billions,* N.Y. Times, Sept. 4, 2003.

[5] Tyler Hamilton, *ID Theft A Click Away,* Toronto Star, May 12, 2003.

[6] FEDERAL TRADE COMMISSION, IDENTITY THEFT SURVEY REPORT 4 (Sept. 2003).

[7] *Id.* at 6.

[8] *Id.* at 6.

understand and address these problems. Frequently, the misuse of personal information is viewed as a technology problem. Indeed, given the ease in which hackers can break into computer systems and data can be intercepted in transmission, there are bound to be significant security problems. As Helen Nissenbaum observes, "[e]xperts in computer security are worried about . . . malicious, avaricious, incompetent, or simply unauthorized outsiders who may break into our online space, damage or steal information, and destroy or compromise our systems."[9] Indeed, many companies use encryption to transmit data securely and fortify their computer systems with firewalls to prevent hackers from gaining access.[10]

However, technology is not the root cause of many abuses of personal information. The shift to a digital environment certainly facilitates information misuse, but at the core, the problem stems from a set of business and government practices. The problem is caused in significant part by the law, which has allowed the construction and use of digital dossiers without adequately regulating the practices by which companies keep them secure. Despite taking elaborate technological measures to protect their data systems, companies readily disseminate the personal information they have collected to a host of other entities and sometimes even to anyone willing to pay a small fee. Companies provide access to their record systems over the phone to anybody in possession of a few easy-to-find pieces of personal information. Even a fortress with impenetrable walls is hardly secure if the back gate is left open.

Reforming this problematic state of affairs requires a rethinking of the way the law comprehends the abuse of personal information. The law fails to focus on the causes of information abuses; it has not identified all the responsible parties; and it has not fashioned appropriate remedies to respond to these abuses. This Essay sketches a new way to think about information abuses, their causes, and the way they should be remedied. Part I examines what I call the "data abuse pyramid." The data abuse pyramid is a way to represent how and why many types of information abuses occur. At the top of the pyramid are actual "misuses" of our data, when information is employed to carry out identity theft, fraud, or other activities. A level below are "leaks" – when entities improperly release or provide access to personal information. And at the bottom is "insecurity," which involves the general lack of protection accorded to our personal data by the entities that hold it. The law attempts to respond at the top of the pyramid, but I contend that to stop information misuses, the law must become involved at the lower levels of the pyramid. In short, the law must address leaks and insecurity. Part II explores how the law can develop to accomplish this task. I recommend ways that existing legal

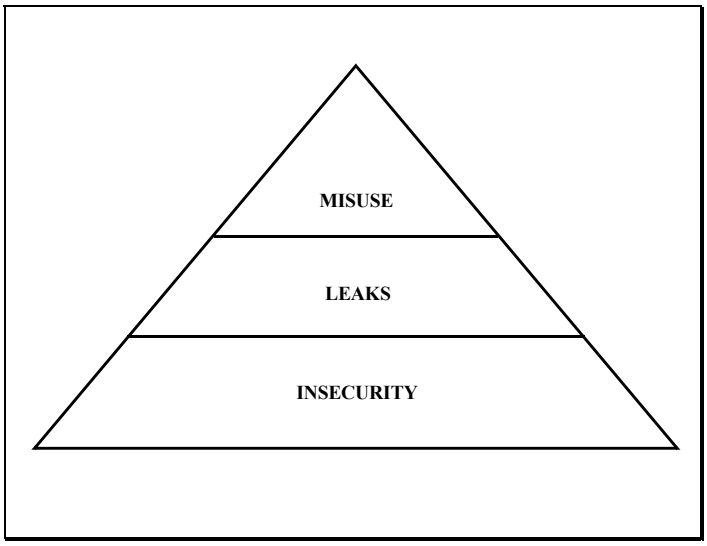
[9] Helen Nissenbaum, *Securing Trust Online: Wisdom or Oxymoron?,* 81 B.U. L. Rev. 635, 659 (2001).

[10] For a discussion of some of the technological solutions to combating certain kinds of digital security problems, see Neal Kumar Katyal, *Digital Architecture as Crime Control,* 112 Yale L.J. 2261 (2003).

concepts can be modified to more effectively redress and deter information abuses.

I. THE DATA ABUSE PYRAMID

To understand the information abuses that are occurring today, we need to understand the data abuse pyramid. The pyramid is meant to be a rather simple model, and it is not designed to represent all information abuses. But it does serve as a useful model for a large percentage of the abuses of our personal data.



There are three levels in the pyramid. I begin with the misuse of personal information, which the law focuses most heavily upon, and I then work my way downward. It is important to distinguish between the different levels of the pyramid because the law responds differently at each level.

A. Misuse

At the top level of the pyramid is the misuse of personal information. Personal data can be misused for identity theft, fraud, stalking, abusive marketing (i.e. spam, telemarketing), and spying on people. These misuses cause concrete injuries – financial losses, emotional distress, and even physical violence.

Identity theft is a nightmare for victims. The identity thief uses a victim's personal information to obtain loans, open fraudulent accounts, and loot existing accounts. As these abuses occur, the victim's dossier becomes polluted with erroneous information – unpaid debts, traffic violations, arrests, and other discrediting data. Because an identity thief impersonates the victim using the victim's personal information, law enforcement databases sometimes associate the victim's name with the thief's criminal activities.

Victims can spend years desperately attempting to fix the destruction wrought by the identity thief.[11] Victims experience great anxiety, leading to psychological harm in certain cases.[12] They have difficulty "obtaining loans, mortgages, security clearances, promotions and even gaining employment."[13] Sometimes, victims are arrested based on warrants for the crimes of the identity thieves.[14] In the words of one victim, "[w]hat has taken me a lifetime to build – my trust, my integrity, and my identity – has been tainted."[15]

In addition to identity thieves, stalkers use personal information to track down people to harass or even kill them. For example, in 1989, a deranged fan brutally murdered actress Rebecca Shaeffer outside her home. He located her home address with the assistance of a private investigator who obtained it from California motor vehicles records.[16]

The law attempts to respond to actual misuses of information. This is because having one's identity stolen, being stalked, or suffering an attack or harassment are all harms that manifest themselves concretely. We can readily comprehend the damage, and we can assess financial losses, physical harm, and emotional trauma. Existing legal responses to data security problems focus on the identity thieves and other criminal miscreants who misuse our information. Indeed, the predominant approach to dealing with identity theft has been to pass new criminal laws.[17] In 1998, Congress passed the Identity Theft and Assumption Deterrence Act making identity theft a federal crime.[18]

However, using the criminal law as the main legal method to combat information abuses has thus far proven ineffective. Law enforcement officials lack enough resources to prosecute identity theft, which is seen as a minor crime when compared to violent crime and drug offenses.[19] Identity thieves are difficult to catch. An identity theft often occurs in many different

---

[11] *See* JANINE BENNER, BETH GIVENS, & ED MIERZWINSKI, NOWHERE TO TURN: VICTIMS SPEAK OUT ON IDENTITY THEFT: A CALPIRG/PRIVACY RIGHTS CLEARINGHOUSE REPORT (May 2000) available at <http://www.privacyrights.org/ar/idtheft2000.htm> [hereinafter "BENNER, NOWHERE TO TURN"].

[12] Christopher P. Couch, Commentary, *Forcing the Choice Between Commerce and Consumers: Application of the FCRA to Identity Theft,* 53 Ala. L. Rev. 583, 586 (2002).

[13] Martha A. Sabol, *The Identity Theft and Assumption Deterrence Act of 1998: Do Individual Victims Finally Get Their Day in Court?*, 11 Loy. Consumer L. Rev. 165, 167 (1999).

[14] U.S. GENERAL ACCOUNTING OFFICE, REPORT TO THE HONORABLE SAM JOHNSON HOUSE OF REPRESENTATIVES, IDENTITY THEFT: GREATER AWARENESS AND USE OF EXISTING DATA ARE NEEDED 23 (June 2002) [hereinafter "GAO IDENTITY THEFT REPORT"]; Lynn M. LoPucki, *Human Identification Theory and the Identity Theft Problem,* 80 Tex. L. Rev. 89, 90 (2001); *see also* Privacy Rights Clearinghouse and Identity Theft Resource Center, *Criminal Identity Theft* (May 2002), http://www.privacyrights.org/fs/fs11g-CrimIdTheft.htm.

[15] Robert O'Harrow, Jr., *Identity Thieves Thrive in the Information Age,* Wash. Post, May 31, 2001, at A1.

[16] See PRISCILLA M. REGAN, LEGISLATING PRIVACY: TECHNOLOGY, SOCIAL VALUES, AND PUBLIC POLICY 102 (1995). The murder of Rebecca Shaeffer led to the passage of the Driver's Privacy Protection Act of 1994, 18 U.S.C. §§ 2721-2725, which restricts the ability of states to disseminate personal information in their motor vehicle records.

[17] GAO IDENTITY THEFT REPORT, supra note XX, at 1.

[18] 18 U.S.C. § 1028.

[19] GAO IDENTITY THEFT REPORT, supra note XX, at 17.

locations, and law enforcement officials "sometimes tend to view identity theft as being 'someone else's problem.'"[20] Most identity theft crimes remain unsolved.[21] In one estimate, less than 1 in 700 instances of identity theft result in a conviction.[22] The focus on criminal law results in inadequate deterrence of identity theft, and it does little to help the victims whose lives are upended.

Victims can attempt to seek redress under tort law, but suing the malefactor who abuses the information will often be futile. The misuser is often too hard to track down and doesn't have deep pockets. Victims can also try to sue the companies from which the information was taken or the companies that enable the thief to set up an account in the victim's name. Although the harm is easy to understand, the law must also recognize that a duty was breached and that this breach caused the harm. These elements are more difficult to establish. The law often views the primary culprit as the thief, the hacker, or the abuser of the data. The companies from which the data is taken are perceived as victims themselves, since they often also suffer financial losses from identity theft.

Even if the law were to view companies that allow improper access to personal information to be at fault, there are still several impediments to a successful suit. It can take a very long time for a concrete injury to materialize. Personal information may be improperly disseminated and only years later will it be used for identity theft.

Furthermore, it is often difficult to trace where an identity thief obtained the personal information used to commit the crime.[23] Many sources hold our personal information. Whereas a stolen piece of physical property can only exist in one location at a time, information can exist in many different hands simultaneously, all of which can spread it further. Unless we can trace where the thief gets her information, it will be difficult to link up a concrete injury to a particular entity that failed to keep data secure. For those companies that allow the identity thief to pollute a victim's dossier – by carelessly granting credit or allowing improper access to an account – it is easier to single out the offending companies. However, there are often many participants that contribute to the harm experienced by identity theft victims: the government agencies and businesses that provide access to the personal information used by the thief, the companies that allow the thief to access and open accounts, the creditors that report the unpaid bills, and the credit reporting agencies that assemble this faulty information and then use it to report on people's reputations. Thieves may obtain information to begin the identity theft from one source, supplement it from other sources, and then go to other companies to obtain credit, open accounts, and obtain credit cards. When the bills are not paid, these companies give damaging information to credit reporting agencies.

---

[20] *Id.* at 18.

[21] Jennifer 8 Lee, *Fighting Back When Someone Steals Your Name,* N.Y. Times, Apr. 8, 2001.

[22] Stephen Mihm, *Dumpster Diving for Your Identity,* N.Y. Times Magazine, Dec. 21, 2003.

[23] Jeff Sovern, *The Jewel of Their Souls: Preventing Identity Theft Through Loss Allocation Rules,* 64 U. Pitt. L. Rev. 343, 398 (2003) ("[C]onsumers may face a causation issue, in that the chain of causation from the disclosure of the consumer's information to the injury to the consumer is a long one.").

This defiles a person's credit reputation, which can harm a person who wants to obtain a mortgage, loan, or job. When the victim attempts to decontaminate her dossier, she is often stymied by uncooperative credit reporting agencies and creditors, and even after the victim manages to go through a time-consuming and lengthy process to clean out the faulty data, more pollution continues to pour into her dossier. The harms of identity theft, therefore, are created through a collaborative effort.

In its most recent attempt to address identity theft, Congress passed the Fair and Accurate Credit Transactions Act (FACTA) in 2003.[24] The FACTA contains some helpful measures to deal with identity theft. People are allowed to request a yearly free credit report from each of the three national credit reporting agencies. FACTA also allows people to opt out of offers of prescreened credit, which are direct mailings that can be intercepted by identity thieves. The Act mandates that when a person places a "fraud alert" in her credit file, the credit reporting agency must contact all the other credit reporting agencies to do likewise. Moreover, the FACTA allows victims to obtain records from businesses that issued credit in their name to an imposter.

Although FACTA makes it somewhat easier for victims to ameliorate the damage caused by identity theft, this is nothing but a better bandaid. Several of FACTA's provisions merely codify what credit reporting agencies had been doing voluntarily, such as contacting the other credit reporting agencies when a fraud alert is placed in a person's file and providing people with free copies of their credit reports. And to counterbalance these benefits, the FACTA preempts more protective state laws. In the end, FACTA does little to make our personal information more secure. Its reforms are remedial, and it fails to proactively prevent identity theft.

How can the law respond more effectively? To do so, the law must better understand and rectify the abuses that occur earlier on before misuses such as identity theft occur.

B. Leaks

The second level of the pyramid involves instances when a company leaks personal information or allows it to be accessed improperly. I refer to this problem as "leaks" because information has been disseminated improperly and it is now somewhere beyond the control of the entity that leaked it. For example, within the past few years, the credit reports of about 13,000 people maintained by Ford Motor Company were accessed illegally.[25] A corrupt employee of a company peddled 30,000 credit reports.[26] The University of Montana website accidentally posted psychological records of over sixty

[24] H.R. 2622 (108th Cong, 1st Sess.) (2003).
[25] Mark Truby, *Ford Credit Discovers ID Theft,* The Detroit News, May 16, 2002
[26] CHRIS JAY HOOFNAGLE, TESTIMONY BEFORE THE SUBCOMM. ON SOCIAL SECURITY OF THE COMM. ON WAYS AND MEANS, U.S. HOUSE OF REPRESENTATIVES, HEARING ON USE AND MISUSE OF THE SOCIAL SECURITY NUMBER (July 10, 2003).

children on the Internet.[27] Leaked information is often a precursor to a misuse such as identity theft. However, there are many instances where information has been leaked without any resulting misuse.

With a leak, the harm consists in being exposed to the potential for being subjected to identity theft, fraud, or even physical danger. People may also suffer anxiety because there is little they can then do to recover the data and prevent downstream abuses of it. However, the law has difficulty in recognizing a harm. The law can at least recognize that a company may have done something wrong. When information is leaked, people may be exposed to a greater risk of identity theft or other abuse even though only a subset of those will actually be victimized. A harm has occurred, since a person is worse off that she would have been before the leak. Nevertheless, many leaks do not result in immediate injury. A concrete injury may never materialize. Or it could happen years later, far beyond any statute of limitations. Until such an injury occurs, the law will not view the situation as ripe for a remedy since the real harm is understood as being the actual misuse of the information, not the mere exposure to the possibility of such misuse. Even if a misuse such as identity theft occurs, it is often hard to trace it to the leaked information.

C. Insecurity

At the bottom of the pyramid is insecurity. Here, the data isn't leaked, but the information security is shoddy. Our digital dossiers can be insecure on numerous fronts. They can be left virtually unlocked for easy access, and they can be left inadequately protected against contamination with false data.

Insecurity is a problem of "architecture." As it is traditionally used, "architecture" refers to the design of physical structures or spaces. Information law scholars, however, have been using the term to describe information infrastructures. Lawrence Lessig and Joel Reidenberg have pointed out that computer systems have an architecture.[28] This architecture is not just a bunch of wires, memory chips, and hard drives, but it also encompasses computer code.

The manner in which data is accessed and used is also an architectural matter. Information systems are designed to grant access to certain people and to deny access to others. For example, an ATM card allows access through possession of the physical card as well as a password (the PIN number). Companies often focus on improving the technological architecture to guard against unauthorized access to their computer networks such as using encryption and firewalls. But the security problems with our digital dossiers are often not caused by invasive technologies or by breakdowns in technological architecture. Rather, these problems are caused by certain practices of the government and businesses.

---

[27] *See* Charles Pillar, *We Mishap: Kids' Psychological Files Posted,* L.A. Times, Nov. 7, 2001.

[28] See LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 5-6, 236 (1999); Joel R. Reidenberg, *Rules of the Road for Global Electronic Highways: Merging Trade and Technical Paradigms*, 6 Harv. J. L. & Tech. 287, 296 (1993).

One such practice involves the degree of supervision and control that a company exercises over its own employees. According to Bruce Schneier, computer security cannot be effective unless the people who use the computers also maintain good security practices.[29] Numerous employees may have access to a database, and some unscrupulous ones may pilfer data for use in identity theft. The FTC has noted the strong growth of "insider threats," where employees funnel data to identity thieves or abscond with information.[30] Another practice that jeopardizes the security of our personal data is the selling of it to others, since all it takes is a weak link in the chain for data security to be seriously compromised.

The central security flaw is the ease by which data can be accessed from the outside through relatively low-tech means. The SSN is at the heart of this problem. Today, SSNs are used as passwords by countless businesses, banks, hospitals, schools, and other institutions to access personal data and accounts.[31] Businesses assume that whoever knows your SSN must be you. Because the SSN is used so frequently by a wide range of institutions as an identifier, it becomes a kind of magic key to our digital dossiers. With an SSN, an identity thief can gain access to a person's existing accounts, apply for credit in the victim's name, open accounts under the name of the victim, and obtain even more information about the victim for further use.[32]

The problem is that the SSN is a terrible password. Numerous people and organizations know our SSN: employers, government agencies, credit reporting agencies, creditors, hospitals, and schools. Since they often are used on ID cards or as driver license numbers, when a person loses her wallet, her SSN is also exposed. SSNs appear on countless documents that inevitably wind their way into the trash to be plucked away by identity thieves.[33] Even if people take the time to shred their trash, thieves can still get their SSNs. The numerous employees at schools, government agencies, and businesses may discard documents with a person's SSN without shredding them. Employees might steal the documents or copy the numbers from the documents. Moreover, SSNs are routinely sold by database companies to any interested buyer.[34] In one instance, an identity thief bought the SSNs of several top corporate executives from database companies.[35] The SSNs of major government officials, including Attorney General John Ashcroft and CIA

---

[29] SCHNEIER, SECRETS AND LIES, *supra* note XX, at 255-269.
[30] Stephen Mihm, *Dumpster-Diving for Your Identity,* N.Y. Times, Dec. 21, 2003.
[31] *See, e.g.,* SIMSON GARFINKEL, DATABASE NATION: THE DEATH OF PRIVACY IN THE 21ST CENTURY 33-34 (2000).
[32] LoPucki, *Identity Theft, supra* note XX, at 104.
[33] Stephen Mihm, *Dumpster-Diving for Your Identity,* N.Y. Times, Dec. 21, 2003.
[34] Robert O'Harrow, Jr., *Identity Thieves Thrive Online,* Wash. Post, May 31, 2001. *See* BETH GIVENS, IDENTITY THEFT: HOW IT HAPPENS, ITS IMPACT ON VICTIMS, AND LEGISLATIVE SOLUTIONS, WRITTEN TESTIMONY FOR THE U.S. SENATE JUDICIARY SUBCOMMITTEE ON TECHNOLOGY, TERRORISM, AND GOVERNMENT INFORMATION 4 (July 12, 2000); Greg Gatlin, *Activists Spur Action Against ID Theft; Social Security Numbers Were for Sale Online,* Boston Herald, Sept. 26, 2003, at 38.
[35] Benjamin Weiser, *Identity Theft, and These Were Big Identities,* N.Y. Times, May 29, 2002.

Director George Tenet were being sold on the Internet for $26 a piece.[36] SSNs are also disclosed in certain public records.[37] As a result of the widespread use of SSNs, anybody who wants to find out our SSN can do so with minimal effort.

Some banks and companies also require people to supply additional information such as addresses, birth dates, or mothers' maiden names.[38] But all this information is often disclosed by the government in public record systems.[39]

Not only does insecurity allow unauthorized access to our personal information, but it results in our dossiers becoming defiled with corrupt information. Credit reporting agencies maintain detailed dossiers about people, which they provide to creditors to assess a person's creditworthiness before offering them a loan.[40] Many employers also examine the credit reports of prospective hires as part of a background check. State licensing entities, such as state bar organizations, often require applicants to submit a credit report. Since credit reporting agencies work only for the creditors and do not establish a relationship with us, we have scant participation in how they use our information, and there are not sufficient market incentives to ensure that a particular person's report is accurate.

Creditors are also to blame, as they often are careless in granting credit. By one estimate, financial institutions mail over three billion pre-approved credit card mailings each year.[41] People can readily apply for instant credit in stores or over the Internet. And they can easily do this in another person's name – all they need is that person's SSN, address, and date of birth. Lynn LoPucki observes that "creditors and credit-reporting agencies often lack both the means and the incentives to correctly identify the persons who seek credit from them or on whom they report."[42]

Therefore, identity theft does not just happen. It has been constructed. The SSN was manufactured by the government. Originally not to be used for identification,[43] it began to be used almost everywhere for just this purpose.[44] Congress recognized the problem in the early 1970s, and passed the Privacy

---

[36] Jennifer C. Kerr, *Bush Aides' Social Security Numbers Sell Cheaply on Net,* Chicago Tribune, Aug. 28, 2003.

[37] Daniel J. Solove, *Access and Aggregation*: *Public Records, Privacy, and the Constitution,* 86 Minn. L. Rev. 1137, 1147 (2002).

[38] Robert O'Harrow, Jr., *Concerns for ID Theft Often Are Unheeded,* Wash. Post, July 23, 2001, at A1.

[39] *See* Solove, *Access and Aggregation, supra* note XX, at 1143-48.

[40] *See* Daniel J. Solove, *Identity Theft, Privacy, and the Architecture of Vulnerability,* 54 Hastings L.J. 1227, 1245 (2003).

[41] BENNER, NOWHERE TO TURN, *supra* note XX at 13.

[42] *Id*. at 94.

[43] ROBERT ELLIS SMITH, BEN FRANKLIN'S WEB SITE: PRIVACY AND CURIOSITY FROM PLYMOUTH ROCK TO THE INTERNET 288 (2000).

[44] *See, e.g.,* UNITED STATES GENERAL ACCOUNTING OFFICE, REPORT TO THE CHAIRMAN, SUBCOMM. ON SOCIAL SECURITY, COMM. ON WAYS AND MEANS, HOUSE OF REPRESENTATIVES: SOCIAL SECURITY: GOVERNMENT AND COMMERCIAL USE OF THE SOCIAL SECURITY NUMBER IS WIDESPREAD (Feb. 1999).

Act of 1974 to restrict the growing use of SSNs as identifiers.[45] But the Act made a critical mistake – it did nothing to restrict the use of the SSN by businesses or other non-government institutions.

This is an architectural system – constructed by the government and by businesses – that makes us all woefully insecure. The government has stamped us with an identification number without providing adequate regulation on its use. Companies routinely allow access to our information with the SSN as a password, which leaves our data virtually undefended. As this discussion has demonstrated, the architectural problem is not in the design of technology, but in the practices for how entities use, disseminate, and provide access to our personal information.

Typically, those discussing information architectures focus on what Lessig calls "architectures of control."[46] Architectures of control are constraining; they are designed to keep people under control. In the early days of the Internet, commentators celebrated its openness and freedom. Lessig, however, saw a more ominous future: "Cyberspace does not guarantee its own freedom but instead carries an extraordinary potential for control."[47] Through computer code and legal code, the Internet can become one of the most controlled places on the planet.

Architectures of control are a serious problem, but architecture works in other troublesome ways. In particular, we are witnessing the increasing construction of what I call "architectures of vulnerability."[48] Whereas architectures of control restrict people's freedom, architectures of vulnerability expose people to a myriad of perils. They sap people of their power.

The key point is that architecture itself can cause harm. If police protection of a neighborhood were taken away, and all the locks to people's homes were removed, this would be a precarious situation to live in, even if nothing happened. Architectures of vulnerability cause harm not only by creating emotional distress and anxiety, but also by increasing our risks of being victimized by identity theft, fraud, stalking, or other crimes. This increased risk is itself a harm.

Unfortunately, the law does little to redress insecurity. Insecurity seems too "soft" to be a cognizable injury. When companies provide incompetent data security, not only has a concrete injury failed to materialize, but also nothing has happened. Hackers haven't hacked it. Identity thieves haven't exploited it. Nothing has been leaked. If somebody leaves the back door ajar, but no burglars come in, then it is difficult for the law to view the situation as ripe for a remedy.

By neglecting to recognize insecurity as a harm, the law is failing in its response to the escalating abuses of personal data. The law is prepared to rectify misuses, but this is often too little, too late. The problem emerges much earlier on – with leaks and inadequate data security. Pursuing the misusers of

---

[45] *Doyle v. Wilson*, 529 F.Supp. 1343, 1348 (D. Del. 1982).
[46] LESSIG, CODE, *supra* note XX, at 30.
[47] *Id*. at 58.
[48] *See* Solove, *Identity Theft, supra* note XX.

information has proven to be ineffectual. To stop the misuse, the law must begin to focus on the locus of the problem – on leaks and insecurity.

II. RETHINKING REMEDIES

Existing legal responses to data security leave the architecture of vulnerability unchanged. They patch up the cracks in the surface, but the foundations remain shaky. The law must shift its focus from the top of the data abuse pyramid (misuse) to the lower levels (leaks, insecurity). Can the law evolve to recognize leaks and insecurity as harms?

A. Shifting the Focus to Security Practices

At the core of the problems with data security is a set of business and government practices. We need to restructure our relationships with businesses and the government with regard to how they treat us when they collect and use our personal data. Currently, the collectors and users of our personal information are frequently not accountable to us. Information is gathered and used; and we have little knowledge and ability to control how secure it remains.

To what extent do the companies that collect and use our personal information owe duties to us? This question remains surprisingly unanswered in the law. However, there are signs that courts are beginning to recognize that the entities using our personal data do have duties to us. For example, in *Remsburg v. Docusearch, Inc.*,[49] a man named Liam Youens bought data about Amy Lynn Boyer from Docusearch, a database company that maintains personal information dossiers on people. Youens requested Boyer's SSN, and Docusearch quickly provided it to him. He then asked for the address of Boyer's employer. Docusearch hired a person to find out by calling Boyer, lying to her about the reason for the call, and inducing Boyer to reveal the address. Docusearch then gave the address to Youens, who went Boyer's workplace and murdered her. The court held that although ordinarily private parties have "no general duty to protect others from the criminal attacks of third parties," where "the defendant's conduct has created an unreasonable risk of criminal misconduct, a duty is owed to those foreseeably endangered."[50] A private investigator "owes a duty to exercise reasonable care not to subject the third person to an unreasonable risk of harm."[51] Therefore, "threats posed by stalking and identity theft lead us to conclude that the risk of criminal misconduct is sufficiently foreseeable so that an investigator has a duty to exercise reasonable care in disclosing a third person's personal information to a client."[52] *Remsburg* is an important step forward in recognizing and remedying modern information privacy harms. *Remsburg* appropriately

[49] 816 A.2d 1001 (N.H. 2003).
[50] *Id.* at 1007.
[51] *Id.* at 1007.
[52] *Id*. at 1008.

recognizes the duty that data collectors and users have to the people whose information they maintain.

Another way to locate duties is by analogizing our relationship with the data collectors and users to a fiduciary one. A fiduciary relationship is one in which a person standing in a special position of power owes special duties to the person subjected to that power.[53] The most famous description of fiduciary duties was penned by Justice Benjamin Cardozo:

> Many forms of conduct permissible in a workaday world for those acting at arm's length, are forbidden to those bound by fiduciary ties. A trustee is held to something stricter than the morals of the market place. Not honesty alone, but the punctilio of an honor the most sensitive, is then the standard of behavior.[54]

In the privacy context, suits have been brought under the tort of breach of confidentiality when personal information is leaked.[55] The virtues of the breach of fiduciary duty approach is that this tort understands the breach to be the harm. Jessica Litman proposes that the breach of confidentiality tort apply to companies that trade in personal information.[56] In particular, she contends, the "reuse, correlation, and sale of consumer transaction data is a straightforward breach of trust."[57] Litman, however, recognizes that the "payoff" of such a tort remedy would be "modest."[58] For Litman, the central problem with common law tort is that it is "gradual and slow" to develop, and "anything so slow is likely to deliver too little, too late."[59] Litman has in mind intentional transfers of data, not data insecurity. However, since fiduciary duties extend beyond a duty of confidentiality, plaintiffs may be able to sue for a breach of a duty to maintain proper data security.

The law of fiduciary relationships is an evolving one. Courts "have carefully refrained from defining instances of fiduciary relations in such a manner that other and perhaps new cases might be excluded."[60] Courts apply a multi-factor analysis to determine whether a fiduciary relationship exists. These factors include: "[T]he degree of kinship of the parties; the disparity in age, health, and mental condition; education and business experience between the parties; and the extent to which the allegedly subservient party entrusted

---

[53] *See* Mobile Oil Corp. v. Rubenfeld, 339 N.Y.S.2d 623, 632 (1972) ("A fiduciary relationship is one founded on trust or confidence reposed by one person in the integrity and fidelity of another. Out of such a relation, the laws raise the rule that neither party may exert influence or pressure upon the other, take selfish advantage of his trust[,] or deal with the subject matter of the trust in such a way as to benefit himself or prejudice the other except in the exercise of utmost good faith.").

[54] Meinhard v. Salmon, 164 N.E. 545, 546 (N.Y. 1928).

[55] McCormick v. England, 494 S.E.2d 431 (S.C. Ct. App. 1997); Biddle v. Warren General Hospital, 715 N.E.2d 518 (Ohio 1999).

[56] See Jessica Litman, *Information Privacy/Information Property,* 52 Stan. L. Rev. 1283, 1304-13 (2000).

[57] *Id.* at 1308.

[58] *Id*. at 1312.

[59] *Id.* at 1312, 1313.

[60] Swerhun v. General Motors Corp., 812 F. Supp. 1218, 1222 (M.D. Fla. 1993).

the handling of . . . business affairs to the other and reposed faith and confidence in [that person or entity]."[61] Courts have likened relationships between patients and physicians as well as attorneys and clients to fiduciary relationships.[62]

The factors generally look for two basic attributes of the relationship: (1) disparities in power; and (2) one party's placing trust in the other party. The first attribute is clearly present in many of our relationships with the companies that gather our personal data. We often lack an ability to bargain over the security of our information and the way it is transferred to others. Moreover, we often are not well informed of the current and potential uses of our information. The second attribute is more complicated. For the companies we do business with, the case is strong. We entrust them with our personal information with the understanding that they will keep it secure. But what about all of the companies that we never do business with that troll about gathering up our data? We don't even have a relationship with these companies. They just take our data—often secretly, without our knowledge.

But the law of fiduciary relationships is a flexible one, and it would not be too much of an expansion of the concept to apply it to the collectors and users of personal information. My argument is not that existing legal doctrine will readily work, but that it has the necessary underlying conceptions to respond to the problem of insecurity. Currently, our relationships to data collectors are perceived to be ones where there is little accountability and responsibility. By rethinking them as more analogous to fiduciary relationships, we will recognize that the collection and use of personal data carries with it profound obligations.

What duties should data collectors and users have? Courts have held that doctors, banks, and schools have a duty to keep personal information confidential.[63] It is not a stretch to conclude that the fiduciary has a duty to keep a person's private information secure. The best source for fiduciary duties of companies that maintain our personal information are the Fair Information Practices. Originally devised in 1973 in a report by the U.S. Department of Housing, Education, and Welfare, the Fair Information Practices consist of a series of principles about rights and responsibilities pertaining to the use of personal data:

> • There must be no personal-data record-keeping systems whose very existence is secret.
> • There must be a way for an individual to find out what information about him is in a record and how it is used.

[61] Pottinger v. Pottinger, 605 N.E.2d 1130, 1137 (Ill. App. 1992).
[62] Hammonds v. Aetna Casualty & Surety Co., 243 F. Supp. 793 (D. Ohio 1965); McCormick v. England, 494 S.E. 2d 431 (S.C. Ct. App. 1997).
[63] McCormick v. England, 494 S.E. 2d 431 (S.C. Ct. App. 1997) (doctor); Peterson v. Idaho First National Bank, 367 P.2d 284 (Idaho 1961) (bank); Blair v. Union Free School District, 324 N.Y.S.2d 222 (N.Y. Dist. Ct. 1971) (school).

> • There must be a way for an individual to prevent information about him obtained for one purpose from being used or made available for other purposes without his consent.
> • There must be a way for an individual to correct or amend a record of identifiable information about him.
> • Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take reasonable precautions to prevent misuse of the data.[64]

If we recognize that the companies that keep our data owe duties to us, then the Fair Information Practices are the most coherent and well-established set of duties for the use of personal data that have been articulated.

Once we change the way we think about the harms caused by insecurity as well as the responsibility companies bear for these harms, then we can bring the law to recognize the most appropriate focal point for responding to information abuses.

B. Tort Remedies Against Businesses

Even if the law concludes that the companies maintaining our personal data bear responsibility for information abuses, it will still be difficult for individuals to pursue remedies. For actual misuses of information, the law will have the least trouble understanding the nature of the harm. As discussed above, however, focusing on misuses will present difficulties because it is often hard to establish a causal connection between specific companies that served as the source of the data used by an information abuser. The most effective tool to improving data security is redressing leaks and insecurity.

One option is to turn to tort law. Under existing tort law, there are at least two theories upon which leaks or insecurity could be recognized as causing cognizable injury. First, leaks or insecurity can cause emotional distress. Second, leaks or insecurity can increase the risk of future harm.

1. Emotional Distress

Leaks or insecurity can cause emotional distress. Of course, the strongest case for emotional distress is when a victim suffers from an actual information misuse. Identity theft causes significant anxiety and emotional trauma when people experience the destruction of their financial reputations. But what about leaks or insecurity? Since most leaks and insecurity are the result of negligence, the tort of negligent infliction of emotional distress would be a potential remedy.

However, courts are especially reluctant to award damages when the emotional distress does not arise out of a more concrete injury, such as bodily

---

[64] U.S. DEP'T OF HEALTH, EDUCATION, AND WELFARE, REPORT OF THE SECRETARY'S ADVISORY COMMITTEE ON AUTOMATED PERSONAL DATA SYSTEMS: RECORDS, COMPUTERS, AND THE RIGHTS OF CITIZENS 41-42 (1973).

harm.[65] Thus, many courts have held that damages for negligent infliction of emotional distress cannot exist alone; they must be accompanied by other physical injuries.[66] For example, in *Doe v. Chao*,[67] the Department of Labor used coal mine workers' SSNs as their identifying numbers for their black lung benefits claims. Administrative law judges issued public hearing notices listing miners' names and SSNs. The judges also used the numbers in their decisions, which were made public.[68] A group of miners sued under the federal Privacy Act. Buck Doe, the lead plaintiff, testified that:

> He was 'greatly concerned and worried' about the disclosure of his SSN; that he felt his privacy had been violated in 'words he cannot describe'; that he felt the consequences of the disclosure of his SSN could be 'devastating' for himself and his wife, and that the disclosure of his SSN had 'torn [him] all to pieces.'[69]

The court held that emotional distress damages cannot be established by a "plaintiff's own conclusory allegations that he felt 'embarrassed,' 'degraded,' or 'devastated,' and suffered a loss of self-esteem."[70] Doe "did not produce any evidence of tangible consequences stemming from his alleged angst over the disclosure of his SSN. He claimed no medical or psychological treatment, no purchase of medications (prescription or over-the-counter), no impact on his behavior, and no physical consequences."[71] The U.S. Supreme Court held that because Doe couldn't establish actual damages, he was not entitled to any liquidated damages under the Privacy Act.[72]

The reason why courts are reluctant to award damages for negligent infliction of emotional distress is that they often view emotional distress damages "with suspicion" because of "concerns over genuineness, reliability, and the specter of unlimited liability for trivial losses."[73] However, the law has made profound progress in recognizing mental and emotional injuries. Originally, the law provided no protection to such harms.[74] Later on, in what became known as the "impact rule," tort law recognized emotional distress damages when the distress arose out of physical injuries.[75] Many jurisdictions expanded the impact rule beyond requiring an initial physical injury to allowing for recovery of emotional distress when it had "physical manifestations."[76] The expansion continued when the law began to permit recovery of emotional distress that arose when a person was not physically

---

[65] JAMES M. FISCHER, UNDERSTANDING REMEDIES 124-25 (1999).
[66] *Id.* at 133.
[67] 306 F.3d 170 (4th Cir. 2002) cert. granted (June 27, 2003).
[68] *Id*. at 175.
[69] *Id.* at 181.
[70] *Id.* at 180
[71] *Id*. at 182.
[72] *See* Doe v. Chao, 124 S. Ct. 1204 (2004).
[73] JAMES M. FISCHER, UNDERSTANDING REMEDIES 124 (1999).
[74] Leslie Benton Sandor & Carol Berry, *Recovery for Negligent Infliction of Emotional Distress Attendant to Economic Loss: A Reassessment,* 37 Ariz. L. Rev. 1248, 1251 (1995).
[75] *Id.* at 1261.
[76] *Id.* at 1261.

injured but was within the "zone of physical danger."[77] The law has taken further steps, allowing recovery for bystanders not within the zone of physical impact who witness loved ones being hurt. In *Dillon v. Legg*,[78] a mother witnessed the death of her daughter in a car accident, but the mother was not in the zone of danger. The court permitted recovery based on negligent infliction of emotional distress. *Dillon* is now followed in many states,[79] but it has strict guidelines that limit recovery based on the plaintiff's observing the event and the relationship between the plaintiff and the injured party.[80] The clear trend is that the law is developing toward easing the restrictions on recovery for emotional harm. Many obstacles to recovery remain, however, and courts are still quite reluctant to recognize emotional distress alone as a cognizable injury.

The difficulty that will plague any form of tort remedy for emotional distress caused by a leak or insecurity is that damages are likely to be small. While many people may experience some anxiety over data leaks and insecurity, it is the rare case where the mental trauma is severe enough to warrant substantial damages. If claims are aggregated, however, a suit may have more punch, and injunctive relief could go far to rectify the problem.

2. Risk of Future Harm

Another potential tort doctrine that might be employed to remedy leaks and insecurity emerges from a growing strain of cases that remedies the creation of a risk of suffering future harm. The potential future harm that a person could suffer from insecurity or leaks includes identity theft, harm to reputation, being hindered in obtaining jobs, loans, or licenses, and emotional distress. *Petriello v. Kalman,*[81] involved a medical malpractice suit in which a physician used excessive suction to remove a fetus that had died in utero. As a result, damage was caused to the plaintiff's intestines, and it required repair with a bowel resection, which involved removing part of the intestine. The plaintiff produced evidence that as a result of this injury, she would have between an 8% to 16% chance that she would suffer a future bowel obstruction.[82] The court noted that under existing law:

> [i]f a plaintiff can prove that there exists a 51 percent chance that his injury is permanent or that future injury will result, he may receive full compensation for that injury as if it were a certainty. If, however, the plaintiff establishes only a 49 percent chance of such a consequence, he may recover nothing for the risk to which he is presently exposed.[83]

---

[77] *Id.* at 1262.
[78] 441 P.2d 912 (Cal. 1968); *see also* Molien v. Kaiser Found. Hospitals, 616 P.2d 813 (Cal. 1980) (permitting recovery for emotional distress not accompanied by physical injuries).
[79] RICHARD A. EPSTEIN, TORTS 276 (1999).
[80] ARTHUR BEST & DAVID W. BARNES, BASIC TORT LAW 536 (2003).
[81] 576 A.2d 474 (Conn. 1990).
[82] *Id*. at 391.
[83] *Id.* at 393.

The court found fault with this system, because it produced an all-or-nothing standard. The result is that "a significant number of persons receive compensation for future consequences that never occur and, conversely, a significant number of persons receive no compensation at all for consequences that later ensue from risks not arising to the level of probability."[84] Therefore, the court concluded that the plaintiff should be compensated for the increased risk of developing the bowel obstruction "to the extent that the future harm is likely to occur."[85]

Courts have begun allowing people to sue for medical malpractice that results in the loss of an "opportunity to obtain a better degree of recovery."[86] Under this approach, the plaintiff "does not receive damages for the *entire* injury, but just for the lost opportunity."[87] In one case, where the doctor argued that the damages were too difficult to calculate, the court concluded that this difficulty should not be a reason to deny recovery and "loss of opportunity is not inherently unquantifiable."[88] Allowing people to recover for potential future harm made more likely by the tortious conduct or the loss of a chance to improve one's condition is a rather new development in tort law, occurring primarily over the past twenty years.[89] Damages can include those "directly resulting from the loss of a chance of achieving a more favorable outcome," as well as damages "for the mental distress from the realization that the patient's prospects of avoiding adverse past or future harm were tortiously destroyed or reduced," and damages "for the medical costs of monitoring the condition in order to detect and respond to a recurrence or complications."[90]

Translated into the domain of information security, tort law would recognize the condition of insecurity as a breach of a duty – a fiduciary one or perhaps an ordinary duty of care. The harm of vulnerability would then be rectified by damages for the increased possibility of harm from identity theft, the mental distress caused by the increased vulnerability, and any costs needed to protect oneself against harms that could arise from the vulnerability.

A problem is that if we applied remedies for insecurity broadly, many kinds of insecurity could potentially become tortious. Suppose that a reckless driver drives aggressively and carelessly, increasing other drivers' potential to be involved in an accident. The law would certainly balk at compensating all of these other drivers for the increased risk. But in other cases the law does remedy increased risk of harm. As illustrated above, the law provides a remedy for increased risk of developing health complications as a result of medical malpractice. One reason for this difference is that once the reckless

---

[84] *Id.* at 394.
[85] *Id.* at 398.
[86] Lord v. Lovett, 770 A.3d 1103, 1105 (N.H. 2001).
[87] *Id.* at 1106.
[88] *Id.* at 1108.
[89] Joseph H. King, Jr., *"Reduction of Likelihood" Reformulation and Other Retrofitting of the Loss-of-Chance Doctrine,* 28 U. Mem. L. Rev. 491, 502 (1998).
[90] *Id.* at 505.

driver passes by, the risk has been survived and is over. In contrast, the risk of developing future complications from medical malpractice is continuing.

Security flaws fit uneasily between these two situations. Unlike medical malpractice, which produces a permanent increased risk of developing a future complication, security flaws can be patched up. This alters the risk of being victimized by data abuse. On the other hand, the risk caused by insecurity is not a once-and-done risk like the reckless driver. It continues until the security flaw is fixed. Thus, upon being sued, a company could reform its data security practices and eliminate the amount of damages a plaintiff could collect. Of course, this is not a total loss to the plaintiff, since bringing the suit can induce a company to improve its practices and the plaintiff may be able to obtain injunctive relief.

3. The Limits and Potential of Tort Law

In sum, these tort doctrines contain the necessary concepts to redress the leak and insecurity harms, but they all have significant limitations and problems to be readily applied. I do not mean to suggest that these difficulties cannot be overcome, but the road will be a rough one. The law of torts will need some creativity and development to be used as a device to induce lasting change in security practices.

In 1890, Samuel Warren and Louis Brandeis attempted to rethink privacy harms and remedies.[91] "[I]n very early times," they contended, "the law gave a remedy only for physical interference with life and property."[92] Subsequently, the law expanded to recognize incorporeal injuries; "[f]rom the action of battery grew that of assault. Much later there came a qualified protection of the individual against offensive noises and odors, against dust and smoke, and excessive vibration. The law of nuisance was developed."[93] Along this trend, the law recognized protection to people's reputations.[94] Furthermore, "[f]rom corporeal property arose the incorporeal rights issuing out of it; and then there opened the wide realm of intangible property, in the products and processes of the mind."[95] Warren and Brandeis were paving the way for the legal recognition of remedies for privacy invasions, which often involve not a physical interference but an "injury to the feelings."[96]

Since the Warren and Brandeis article, the law has come a long way in recognizing privacy harms. Among other things, people can find legal redress for disclosures of embarrassing true information about their private lives, for intrusions into their seclusion and solitude, and for a host of other types of harms.[97] Today, new abuses such as leaks and insecurity are becoming more prevalent, and they are currently not well-recognized by the law. Tort law is

---

[91] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).
[92] *Id*. at 193.
[93] *Id.* at 194.
[94] *Id.* at 194.
[95] *Id.* at 194.
[96] *Id.* at 197.
[97] *See* RESTATEMENT (SECOND) OF TORTS §§ 652B (intrusion); 652D (public disclosure).

much more advanced than it was in Warren and Brandeis' day. Basic underlying concepts are in place, and the law even partially recognizes the kinds of harms that leaks and insecurity create. The critical question, then, is whether tort law will take the next step.

C. Constitutional Remedies Against the Government

With regard to the data practices of the government, the constitutional right to information privacy could conceivably provide a remedy. In *Whalen v. Roe,*[98] the Court concluded that the right to privacy protects not only "independence in making certain kinds of important decisions" but also the "individual interest in avoiding disclosure of personal matters."[99] The case involved a government record system of individuals who were taking prescriptions for certain medications. Although the government promised that the information was confidential and secure, the plaintiffs contended that they feared the possibility of the information leaking out. The Court concluded that because the security was adequate, the state had met its constitutional obligations. In a key passage in the case, the Court stated:

> We are not unaware of the threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files. . . . The right to collect and use such data for public purposes is typically accompanied by a concomitant statutory or regulatory duty to avoid unwarranted disclosures. . . . [I]n some circumstances that duty has its roots in the Constitution.[100]

Therefore, according to the Court in *Whalen,* when the government maintains personal information, it has the responsibility to keep it secure.

The constitutional right to information privacy is a work in progress. Although the Supreme Court has done little to develop it, the right has been recognized in a majority of circuit courts.[101] Therefore, the constitutional right to information privacy has the potential to develop into a way for people to ensure that the government keep their information secure. People can bring *Bivens* or §1983 actions for damages and injunctions. In this way, the

---

[98] 429 U.S. 589 (1977).
[99] *Id.* at 599-600.
[100] *Id*. at 605.
[101] After *Whalen* and *Nixon*, the Court has done little to develop the right of information privacy. As one court observed, the right "has been infrequently examined; as a result, its contours remain less than clear." *Davis v. Bucher*, 853 F.2d 718, 720 (9th Cir. 1988). Most circuit courts have recognized the constitutional right to information privacy. *See, e.g.*, United States v. Westinghouse Electric Corp., 638 F.2d 570, 577-580 (3d Cir.1980); Plante v. Gonzalez, 575 F.2d 1119, 1132, 1134 (5th Cir.1978); Barry v. City of New York, 712 F.2d 1554, 1559 (2d Cir.1983); In re Crawford, 194 F.3d 954, 959 (9th Cir. 1999); J.P. v. DeSanti, 653 F.2d 1080, 1089 (6th Cir.1981); Walls v. City of Petersburg, 895 F.2d 188, 192 (4th Cir. 1990); *but see* American Federation of Government Employees, AFL-CIO v. Department of Housing & Urban Development, 118 F.3d 786, 191-92 (D.C. Cir. 1997) (expressing "grave doubts" as the existence of the right but not directly addressing the issue of the existence of the right).

constitutional right to information privacy can work as a tort action against the government for shoddy security. It can also limit the extent to which the government permits public access to personal information.

States that do not adequately account for privacy in their public record laws may be found to violate the constitutional right to information privacy. Since some of the personal information disclosed in public record systems can facilitate the commission of identity theft and other misuses, it can compromise a person's security. For example, one court clerk in Cincinnati placed an entire county's court records on the Internet. A person whose speeding ticket was posted on the website had his identity stolen because the ticket contained a treasure trove of personal information, including the person's SSN.[102]

At least one court has recognized that the dissemination of information in public records can implicate the constitutional right to information privacy. In *Kallstrom v. City of Columbus*,[103] a city disclosed law enforcement officials' personnel files to defense counsel of alleged drug conspirators (whom the officials had investigated). The personnel files included the officer's names, addresses, phone numbers, financial information, Social Security numbers, and responses to questions about their personal life as well as the names, addresses, and phone numbers of immediate family members.[104] The city disclosed to avert a violation of Ohio's Public Records Act, which makes records available to the public unless the record falls within an enumerated exemption. The Act did not have a privacy exemption. The court held that the disclosures created a serious risk to the "personal security and bodily integrity" of the plaintiffs and their families.[105] Applying strict scrutiny, the court held that the disclosure violated the constitutional right to information privacy because it did not further the public's understanding of law enforcement agencies.[106]

Therefore, the constitutional right to information privacy imposes upon the government a responsibility to keep the data it collects secure and confidential absent an overriding consideration on the other side of the scale. However, this way of applying the constitutional right to information privacy may meet resistance in the courts, especially given the germinal and uncertain status of the right.

D. Structural Remedies

Insecurity harms are difficult to rectify with individual tort suits, since damages are harder to establish and people are often given so little information about a company's security practices that it will be difficult for them to find out enough to bring a suit. Therefore, the most effective means for reforming the architecture must be more systematic than what individual remedies can

[102] Jennifer 8. Lee, *Dirty Laundry, Online for All to See,* N.Y. Times, Sept. 5, 2002, at G1.
[103] 136 F.3d 1055 (6th Cir. 1998).
[104] *Id.* at 1059.
[105] *Id.* at 1062.
[106] *Id.* at 1065.

provide. Although I believe individual remedies are an important tool, a system of regulation will be better able to improve security at a more global level. Information security must be regulated by an national agency with the appropriate expertise to understand information privacy issues.

Thus far, the FTC has been attempting to develop such a regulatory system. Beginning in 1998, the Federal Trade Commission (FTC) has been expanding its reach by bringing actions against businesses that breach their own privacy policies. According to the FTC, such a breach is an "unfair or deceptive acts or practices in or affecting commerce."[107] Armed with the power to bring civil actions and obtain injunctions, the FTC has initiated a number of cases, practically all resulting in settlements.[108] Several of these cases involved improperly disclosed or leaked data.

There are indications that the FTC is expanding its reach beyond leaks to insecurity harms. In particular, the FTC charged Microsoft's Passport, which allows Internet users to use a single username and password to log in to a variety of participating websites, was not providing adequate security, which it had promised in its privacy policy. Microsoft settled with the FTC, and it promised to improve its security.[109] The Passport case marks a very important new development in FTC enforcement. The FTC appears to have recognized security harms as cognizable. In another recent case, *In re Guess.com, Inc.,*[110] the FTC brought an action against Guess for having shoddy security for its customers' personal data in violation of its privacy policy.

There are many reasons to remain skeptical about the FTC's ability to develop into the kind of national privacy agency needed to reform the security of our digital dossiers. The FTC's jurisdiction is limited, and the enforcement of privacy is not its primary mission.[111] Another limitation with the FTC is that it thus far only ensures that companies follow the promises they make in their privacy policies.[112] But there is a way around this limitation contained in a little-known provision of the Gramm-Leach-Bliley (GLB) Act. The GLB Act requires the various agencies that regulate financial companies to enact "administrative, technical, and physical safeguards for personal information."[113] These regulations promulgaged under the GLB Act are rather vague, but they could be used to enable agencies such as the FTC to bring actions to force companies to abandon the use of SSNs and other readily available personal information as passwords. Unfortunately, this kind of insecurity has not been recognized by the FTC. The focus on information security has thus far been centered around technology, not around these basic business practices that allow easy access to personal data.

---

[107] 15 U.S.C. § 45.
[108] See DANIEL J. SOLOVE & MARC ROTENBERG, INFORMATION PRIVACY LAW 541-553 (2003).
[109] *See In the Matter of Microsoft Corp.,* No. 012-3240.
[110] No. 022-3260 (July 30, 2003).
[111] *See* Joel R. Reidenberg, *Privacy Wrongs in Search of Remedies,* 54 Hastings L.J. 877, 888 (2003).
[112] *See* Paul M. Schwartz, *Privacy and Democracy in Cyberspace,* 52 Vand. L. Rev. 1609, 1638 (1999).
[113] 15 U.S.C. §§ 6801(b); 6805(b)(2).

III. CONCLUSION

We are increasingly vulnerable in the Information Age, and the information abuses we are experiencing are the product of business and the government. We need to rethink information abuses by understanding insecurity as a cognizable injury and focusing more on the companies maintaining and using our personal information. The most effective approach to dealing with information abuses is to focus on the bottom of the data security pyramid, not the top.