Hastings Law Journal

Volume 54 | Issue 4 Article 9

1-2003

Identity Theft, Privacy, and the Architecture of Vulnerability

Daniel J. Solove

Follow this and additional works at: https://repository.uchastings.edu/hastings_law_journal

 Part of the Law Commons

Recommended Citation

Daniel J. Solove, *Identity Theft, Privacy, and the Architecture of Vulnerability*, 54 Hastings L.J. 1227 (2003).
Available at: https://repository.uchastings.edu/hastings_law_journal/vol54/iss4/9

This Article is brought to you for free and open access by the Law Journals at UC Hastings Scholarship Repository. It has been accepted for inclusion in Hastings Law Journal by an authorized editor of UC Hastings Scholarship Repository.

Identity Theft, Privacy, and the Architecture of Vulnerability

by
DANIEL J. SOLOVE*

INTRODUCTION **1228**

I. ARCHITECTURE AND THE PROTECTION OF PRIVACY **1229**

A. THE TRADITIONAL MODEL 1229
B. ARCHITECTURE 1238

II. RECONCEPTUALIZING IDENTITY THEFT **1243**

A. THE IDENTITY THEFT PROBLEM 1243
B. IDENTITY THEFT AND THE TRADITIONAL MODEL 1246
C. IDENTITY THEFT AS ARCHITECTURE 1251

III. FORGING A NEW ARCHITECTURE **1261**

A. THE PROBLEM WITH IDENTIFICATION SYSTEMS 1262
B. A NEW ARCHITECTURE: PARTICIPATION AND RESPONSIBILITY 1266
(1) Participation *1268*
(2) Responsibility *1269*
(a) Existing Accounts and Data Holders 1269
(b) New Accounts 1271
(3) Foundations *1272*

CONCLUSION **1275**

* Assistant Professor, Seton Hall Law School; J.D. Yale, 1997. Thanks to Beth Givens, Linda Folely, Lynn LoPucki, Marc Rotenberg, Paul Schwartz, Richard Sobel, and Charles Sullivan for their very helpful comments on the manuscript. John Spaccarotella provided excellent research assistance. The Seton Hall Law School faculty scholarship fund provided financial support for this project.

Introduction

Traditionally, privacy violations have been understood as invasive actions by particular wrongdoers who cause direct injury to victims. Victims experience embarrassment, mental distress, or harm to their reputations. Privacy is not infringed until these mental injuries materialize. Thus, the law responds when a person's deepest secrets are exposed, reputation is tarnished, or home is invaded. Under the traditional view, privacy is an individual right, remedied at the initiative of the individual.

This way of understanding privacy and the manner in which it should be protected is being severely challenged by the privacy problems arising in today's Information Age. These are problems involving the flow of information: the construction of detailed digital dossiers about people; the increasing accessibility of personal information; the growing use of personal information to make important decisions affecting people's lives; the widespread transfer of information between a variety of entities; the burgeoning expansion in different uses for personal data; and the emerging collaboration between private sector entities gathering personal data and government law enforcement officials. These problems are of a different character than traditional privacy problems, and they must be conceptualized and protected against differently.

Protecting privacy starts with conceptualizing privacy. We need to understand the nature of privacy problems in order to solve them. In this Article, I contend that many of these emerging privacy problems must be understood "architecturally" as part of a larger social and legal structure. Consequently, protecting privacy must focus not merely on remedies and penalties but on shaping architectures. I argue that many of the privacy problems posed by the Information Age cannot adequately be remedied by individual rights and remedies alone.

In Part I, I employ the notion of architecture to describe a different way of understanding certain privacy problems and how the law should protect against them.

In Part II, I illustrate these points with the example of identity theft, one of the most rapidly growing types of criminal activity.[1] A criminal impersonates an individual by using personal data to obtain accounts, credit cards, and loans. This upends a person's life, destroys her credit, and often prevents her from engaging in important

1. *See* Robert O'Harrow, Jr., *Identity Thieves Thrive in Information Age; Rise of Online Data Brokers Makes Criminal Impersonation Easier*, WASH. POST, May 31, 2001, at A1.

activities such as making purchases, obtaining loans or mortgages, renting an apartment, or even getting a job or license.

Identity theft is often conceptualized as the product of disparate thieves and crafty criminals. The problem, however, has not been adequately conceptualized, and, as a result, enforcement efforts have been misdirected. The problem, as I contend, is one created by an architecture that is deeply flawed. Understanding identity theft in terms of architecture reveals that it is part of a larger problem that the law has thus far ignored.

I. Architecture and the Protection of Privacy

A. The Traditional Model

The question of how to protect privacy was of paramount importance to Samuel Warren and Louis Brandeis in 1890, when they wrote their profoundly influential article, *The Right to Privacy*.[2] The authors raised great concern about new technologies for photography which would make taking photographs significantly easier and cheaper.[3] These technological developments intersected with a rapidly growing press, which was becoming increasingly sensationalistic. "Of the desirability—indeed of the necessity—of some such protection [of privacy], there can, it is believed, be no doubt."[4] The problem facing Warren and Brandeis was that the common law in 1890 did not provide much protection for privacy.

Around the same time Warren and Brandeis wrote their article, E.L. Godkin, a famous social commentator of his day,[5] also observed that privacy was being endangered by the excessive exploits of the press. Godkin was not optimistic about the possibility of a legal solution to these new threats to privacy:

> In truth, there is only one remedy for the violations of the right to privacy within the reach of the American public, and that is but an imperfect one. It is to be found in attaching social discredit to invasions of it on the part of conductors of the press. At present this check can hardly be said to exist.[6]

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

3. *Id.* at 195–96.

4. *Id.* at 196.

5. *See* Elbridge L. Adams, *The Right to Privacy and its Relation to the Law of Libel*, 39 AM. L. REV. 37 (1905); Dorothy J. Glancy, *The Invention of the Right to Privacy*, 21 ARIZ. L. REV. 1 (1979).

6. E.L. Godkin, *The Rights of the Citizen: IV. To His Own Reputation*, SCRIBNER'S MAGAZINE, 1890, at 67; *see also* E.L. Godkin, *The Right to Privacy*, THE NATION, Dec. 25, 1890, at 496–97.

Unlike Godkin, Warren and Brandeis believed that law could solve these privacy problems. Warren and Brandeis argued that existing legal causes of action did not adequately protect privacy but that legal concepts in the common law could be modified to protect privacy effectively. The common law had the necessary foundations for protecting privacy, for it "secures to each individual the right of determining, ordinarily, to what extent his thoughts, sentiments, and emotions shall be communicated to others."[7] This right "is merely an instance of the enforcement of a more general right of the individual to be let alone."[8] From this more general right, the authors concluded, protections against privacy violations could be derived in the common law.[9]

What Warren and Brandeis achieved was nothing short of magnificent. By pulling together various isolated strands of the common law, the authors demonstrated that the law contained the seeds of remedies for privacy invasions. They illustrated why creating these remedies would not constitute a radical addition to the common law but would merely be an extension and an elaboration of what was already germinating.[10]

Warren and Brandeis discussed three remedies to protect privacy. First, they contended that invasions of privacy should give rise to "[a]n action of tort for damages in all cases."[11] Regarding damages, "[i]f the invasion of privacy constitutes a legal *injuria,* the elements for demanding redress exist, since already the value of mental suffering, caused by an act wrongful in itself, is recognized as a basis for compensation."[12] Therefore, Warren and Brandeis's primary enforcement mechanism consisted of tort damages to compensate individuals for the "mental suffering" caused by privacy invasions. Second, in a "very limited class of cases," an injunction might be appropriate.[13] Third, with legislation, criminal penalties can be imposed "within narrower limits."[14]

Warren and Brandeis's understanding of privacy problems has been highly influential in the development of privacy law, and I will refer to this understanding as the "traditional model." Under this model, privacy is understood as a series of discrete wrongs to specific individuals. These wrongs occur through the actions of particular

7. Warren & Brandeis, *supra* note 2, at 198.

8. *Id.* at 205.

9. *Id.*

10. *Id.* at 206, 213 n.1 ("The application of an existing principle to a new state of facts is not judicial legislation.").

11. *Id.* at 219.

12. *Id.* at 213.

13. *Id.* at 219.

14. *Id.*

wrongdoers. The injury is experienced by the individuals who are wronged. For example, a privacy violation that would fit well into the traditional model is a newspaper publishing a photograph of a person in the nude. There is a particular wrongdoer (the newspaper) that engages in a particular action (publishing the photograph) which causes harm to a particular individual. This harm consists of mental distress and any consequent physical or mental impairment.

Under the traditional model, privacy protections safeguard against these wrongs to individuals. Protection consists of rights and remedies for each instance of harm, and in certain cases, criminal punishments for the wrongdoers. Thus, the traditional model is reactive. It waits for harms to materialize in concrete form and then reacts. The traditional model works to prevent future harms through the deterrent effects of civil liability and criminal penalties.

Another aspect of the traditional model is that it often views privacy protections in the form of rights possessed and remedied at the initiative of individuals. The value of protecting privacy is measured in terms of the value of preventing harm to the individual. Privacy is treated as an individual entitlement. In the words of one court, "[p]rivacy is inherently personal. The right to privacy recognizes the sovereignty of the *individual.*"[15] According to the Restatement of Torts: "The right protected by the action for invasion of privacy is a personal right, peculiar to the individual whose privacy is invaded."[16] Under this view, privacy is enforced by providing individuals with remedies for privacy invasions. For example, each of the four privacy torts, inspired by Warren and Brandeis's 1890 article,[17] affords a remedy to specific harms caused to specific individuals. The tort of intrusion upon seclusion protects against the intentional intrusion into an individual's "solicitude or seclusion" or "his private affairs or concerns."[18] The public disclosure of private facts tort provides individuals with remedies against publicly revealing matters concerning their private lives.[19] The tort of false light protects individuals against the dissemination of false information.[20] And the tort of appropriation protects individuals from the use of their name or likeness for the benefit of another person or entity.[21]

The privacy torts are designed to redress specific harms. In many cases however, damages are likely to be small, thus creating little

15. Smith v. City of Artesia, 772 P.2d 373, 376 (N.M. Ct. App. 1989).
16. RESTATEMENT (SECOND) OF TORTS § 652I comment (a)(1977).
17. Warren & Brandeis, *supra* note 2, at 196.
18. RESTATEMENT (SECOND) OF TORTS § 652B (1977).
19. *Id.* § 652D.
20. *Id.* § 652E.
21. *Id.* § 652C.

incentive to sue. The result is that privacy is most protected in situations where damages can be defined palpably, such as where skeletons in the closet are revealed, where nudity is publicly disclosed, or where the press sneaks into a person's home to obtain personal information.

Like tort law, criminal law focuses on specific wrongdoers. It aims to deter crime by establishing penalties for privacy invasions. Criminal law is often reactive, responding to crime with punishment after its occurrence. Frequently, criminal law fails to be proactive in preventing crime. Although criminal law certainly works to deter crime, some crimes are difficult to deter. Criminal law can only reach a certain level of deterrence, which can be limited by difficulties in catching and prosecuting the perpetrators. Crimes involving the use and dissemination of personal information present complicated enforcement problems, since these crimes can occur from anywhere in the world, are easy to conceal, and take a long time to detect.

Although the traditional model works for a number of privacy problems, not all privacy problems are the same, and many privacy problems do not fit well into this model. Elsewhere, I contended that privacy is not a unitary concept.[22] I argued that privacy cannot be adequately conceptualized by isolating a common denominator in all of the multifarious things we understand as implicating privacy. Instead, privacy should be conceptualized from the bottom-up, by focusing on particular problems which are related but do not necessarily share one element in common. There are many different types of privacy problems, and although related, they differ in significant ways.

The traditional model does not adequately account for many of the privacy problems arising today. A number of privacy problems do not consist merely of a series of isolated and discrete invasions or harms, but are systemic in nature. Although I have argued that privacy must be understood contextually and that privacy problems have differences which should be more carefully examined,[23] this does not mean that privacy is invaded only through a series of singular incursions. In certain contexts, the privacy harm is caused by a particular social or legal structure, not by a few isolated actors.

Many modern privacy problems are systemic in nature. They are the product of information flows, which occur between a variety of different entities. There is often no single wrongdoer; responsibility is spread among a multitude of actors, with a vast array of motives and aims, each doing different things at different times. For example, when a person unwittingly finds herself embroiled in a public news

22. Daniel J. Solove, *Conceptualizing Privacy*, 90 CAL. L. REV. 1087, 1092 (2002).
23. *Id.* at 1126–43.

story, the invasiveness of the media is often not the product of one particular reporter. Rather, the collective actions of numerous reporters camping outside one's home and following one wherever she goes severely disrupt her life. The difficulty in obtaining a legal remedy for this disruption is that no one reporter's actions may be all that invasive or objectionable. The harm is created by the totality of privacy invasions, but the tort of intrusion upon seclusion only focuses on each particular actor.[24]

Today, much modern information gathering occurs in piecemeal fashion. A difficulty I have described as the "aggregation problem" complicates the application of tort law in specific cases.[25] In isolation, a particular piece of information may not be very invasive of one's privacy. But when pieces of information are combined, they may form a detailed account of an individual, what I have referred to as a "digital biography."[26] The whole may be greater than the sum of the parts. This phenomenon occurs because information that is not revealing alone can be quite revealing in combination with other pieces of information.

Further, the trade of personal information between private sector entities today is not readily analogous to the widespread disclosure of information by the media. Entities often buy and sell information, resulting in the disclosure of that information to only a few other entities. It is difficult to assess damages when one company maintains a database about a person and sells that information to other companies or the government.[27] These harms do not translate well to tort law or criminal law, which focus on isolated actors and address harms individually rather than collectively.

The traditional view of privacy harms pervades much of the law of information privacy. Courts often look for specific injuries. For example, in *U.S. West, Inc. v. Federal Communications Commission*,[28] the court struck down regulations of the Federal Communications

24. As Bruce Sanford contends: "A stake-out by a group of unrelated reporters should be viewed as no more than the sum of its separate parts." BRUCE W. SANFORD, LIBEL AND PRIVACY § 11.2, at 541 (2d ed. 1991) (Supp. 2003).

25. Daniel J. Solove, *Access and Aggregation: Public Records, Privacy, and the Constitution*, 86 MINN. L. REV. 1137, 1184–95 (2002) [hereinafter *Access*]; Daniel J. Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 STAN. L. REV. 1393, 1434 (2001) [hereinafter Solove, *Privacy*].

26. *See Access, supra* note 25, at 1184–95.

27. Certain more modern privacy laws—namely, a number of the statutes passed since the 1970s—have minimum damages provisions, eliminating the difficult task of proving specific harm. *See, e.g.*, The Electronic Communications Privacy Act, 18 U.S.C. § 2511(4)(a) (1993) (minimum $10,000 per violation); 18 U.S.C. § 2710(c) (West 1993) (liquidated damages of $2500). Nevertheless, these laws often still suffer from other problems in the traditional model, discussed below.

28. 182 F.3d 1224 (10th Cir. 1999).

Commission ("FCC") requiring that consumers opt-in before telecommunications carriers could use or disclose their personal information. The court reasoned that the governmental interest in protecting privacy was not "substantial" because the government failed to "show that the dissemination of the information desired to be kept private would inflict specific and significant harm on individuals, such as undue embarrassment or ridicule, intimidation or harassment, or misappropriation of sensitive personal information for the purposes of assuming another's identity."[29] This way of viewing the harm to privacy fails to acknowledge the larger systemic problems involved with information flow. These problems affect the type of world we are creating. As I have discussed at length elsewhere, the growing use and dissemination of personal information creates a Kafkaesque world of bureaucracy, where people are increasingly powerless and vulnerable, where personal information is not only outside our control but also is subjected to a bureaucratic process that is itself not adequately controlled.[30] This generalized harm already exists; we need not wait for specific abuses to occur.

Enforcement at the initiative of the individual also creates difficulties. Arguing from the traditional model, Fred Cate contends that although people claim they desire more privacy, their actions illustrate that they do not want to sacrifice much time or energy in obtaining it.[31] The goal of the law, says Cate, should be to assist those who want to protect their privacy rather than to thrust a uniform wall of privacy around everyone: "The law should serve as a gap-filler, facilitating individual action in those situations in which the lack of competition has interfered with private privacy protection."[32] Furthermore, according to Cate, the purpose of privacy rights is to "facilitate . . . the development of private mechanisms and individual choice as a means of valuing and protecting privacy."[33]

However, many privacy problems cannot be adequately redressed by relying on individual initiative alone. As Paul Schwartz argues, affording individuals a right to control their personal data improperly assumes that individuals have the ability to exercise meaningful control over their information.[34] Schwartz calls this problem the "autonomy trap."[35] Schwartz notes how consent screens

29. *Id.* at 1234–35.

30. Solove, *Privacy*, *supra* note 25, at 1399.

31. FRED H. CATE, PRIVACY IN THE INFORMATION AGE 196 (1997).

32. *Id.* at 131.

33. *Id.*

34. Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1661–64 (1999) [hereinafter *Privacy and Democracy*]; *see also* Paul M. Schwartz, *Internet Privacy and the State*, 32 CONN. L. REV. 815 (2000) [hereinafter *Internet*].

35. *Privacy and Democracy*, *supra* note 34, at 1660.

on a website asking users to relinquish control over information often do so on a "take-it-or-leave-it basis" resulting in the "fiction" that people have "expressed informed consent to [the website's] data processing practices."[36] Stated more broadly, there are a number of forces that prevent individuals from exercising their preferences to protect their privacy.

For example, a person may want to purchase books from an online bookseller. Suppose that the person's privacy preferences consist of the information being kept very secure, not being disclosed to the government, and not being traded or disclosed to other companies (even in the event that the company goes bankrupt). But the online bookseller's privacy policy is standardized and often does not address these points with any reasonable degree of specificity. The policy contains a blanket statement that information is kept secure, but there are not enough details for the person to make an accurate assessment of the level of security. The policy says nothing about the bookseller's policies regarding government access to personal information. If the bookseller were issued a subpoena for the person's data, would the bookseller oppose it? Would the bookseller inform the person beforehand? These questions are unanswered.[37] Finally, the policy says that in the event the company goes bankrupt, information may be among the transferred assets. And since privacy policies are remarkably similar among many companies, many other online bookstores offer similar terms. If the person decides to purchase the book in a bricks-and-mortar bookstore, she faces the same difficulties if she pays by credit card.[38] There, the privacy policies are not even readily available to the purchaser. In short, there is not a lot of bargaining over privacy. This state of affairs exists partly because there are not many choices available to people regarding their privacy and because people are often not aware of the problems, risks, and dangers about how their information is handled. Even if they were, it is doubtful whether a person could create a special deal with a company to provide greater protections for her privacy. With regard to the level of privacy protection offered by companies, a person must simply take it or

36. *Id.* at 1662.

37. See Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083, 1099–1100 (2002), for a discussion of the inadequacies of privacy policies in informing people about government access to their personal information.

38. This is illustrated by Kenneth Starr's subpoena of Kramerbooks for records about Monica Lewinsky's book purchases. *See* Felicity Barringer, *Using Books as Evidence Against Their Readers*, N.Y. TIMES, Apr. 8, 2001, at WK3. In that case, Kramerbooks decided to challenge the subpoena, but the bookstore was not under any obligation to do so.

leave it. People are not afforded enough choices to exercise their privacy preferences. Because companies controlling personal information are secretive about its uses and vague about their privacy policies, people lack adequate knowledge to make meaningful choices.

Placing the onus on individuals to protect their privacy, as Cate recommends, can only be effective if individuals have the power to exercise their rights. Enforcement mechanisms that rely upon individual initiative often fail because individuals lack the knowledge, power, and resources to use them. Toni Morrison's *The Bluest Eye* vividly illustrates this point. The novel chronicles the tragic life of Pecola Breedlove, an African-American girl growing up in a poor and abusive family. Pecola considers herself ugly and dreams of having blue eyes. The Breedloves live amid dinginess and squalor in an abandoned store, which they have partitioned into rooms. The Breedloves are radically disempowered. All of the rights and legal protections afforded to people in this country have little effect on their lives. For example, the Breedloves purchase a new sofa, which they receive in severely damaged condition. Cholly Breedlove, Pecola's father, futilely attempts to complain:

> [The sofa] had been purchased new, but the fabric had been split straight across the back by the time it was delivered. The store would not take the responsibility. . . .
>
> "Looka here, buddy. It was O.K. when I put it on the truck. The store can't do anything about it once it's on the truck. . . ." Listerine and Lucky Strike breath.
>
> "But I don't want no tore couch if'n it's bought new." Pleading eyes and tightened testicles.
>
> "Tough shit, buddy. *Your* tough shit. . . ."
>
> You could hate a sofa, of course—that is, you could hate a sofa. But it didn't matter. You still had to get together $4.80 a month. If you had to pay $4.80 a month for a sofa that started off split, no good, and humiliating—you couldn't take any joy in owning it. And the joylessness stank, pervaded everything. The stink of it kept you from painting the beaverboard walls; from getting a matching piece of material for the chair; even from sewing up the split, which became a gash, which became a gaping chasm that exposed the cheap frame and cheaper upholstery. It withheld the refreshment in a sleep slept on it. . . .[39]

The Breedloves accept the torn couch even though it is clear that the law affords them a remedy. However, the Breedloves are unaware of the legal remedies they might have and they lack the ability to bring a lawsuit. This example illustrates that rights,

39. TONI MORRISON, THE BLUEST EYE 36 (1998).

remedies, and legal protections can only be effective if people have the power to use them. The Breedloves are powerless because they have been trained to be powerless; they accept whatever injustice comes their way because they have come to learn that this is the lot life continually deals them.

In an interesting contrast, especially to Pecola, stands the character of Maureen Peal. Maureen is a new African-American girl in Pecola's school, and she is nicely dressed, rich (relative to the other girls), popular, and self-confident. Maureen has "enchanted the entire school" and has a "rich autumn ripeness in her walk."[40] In one scene, Maureen describes an instance where her uncle sued an ice cream store that refused to serve him:

> "My uncle sued Isaley's," Maureen said to the three of us. "He sued the Isaley's in Akron. They said he was disorderly and that that was why they wouldn't serve him, but a friend of his, a policeman, came in and beared the witness, so the suit went through."
>
> "What's a suit?"
>
> "It's when you can beat them up if you want to and won't anybody do nothing. Our family does it all the time. We believe in suits."[41]

In contrast to the Breedloves, Maureen Peal has considerable power because she has a very different mindset. The Peal family members are aware of their legal rights and are able to use the legal system effectively. They have the financial resources to do so, as well as the assistance of a policeman whose testimony was essential to the success of Maureen's uncle's lawsuit.

These scenes from *The Bluest Eye* illustrate a profound problem with individual remedies—they are only effective to the extent that individuals have power to exercise them. Individual remedies are often powerless in the face of larger forces created by social structure. A person may have the legal opportunity to bargain to modify a contract, lease, or employment agreement or to sue for redress if wronged. But unless that person has the knowledge and ability to bargain or to sue, the opportunities are often not very empowering.

If we afford privacy rights, we must do so in a system where they can be meaningfully exercised. Rights to consent to the collection of data also lack much meaning if people can be readily pressured, mislead, or coerced into relinquishing their information.[42] Anita Allen notes that people readily surrender their privacy, and privacy

40. *Id.* at 62.

41. *Id.* at 68.

42. *See* Schwartz, *Privacy and Democracy*, *supra* note 34, at 1660–64; Solove, *Privacy*, *supra* note 25, at 1453–54.

expectations are eroding.[43] According to Allen, "[p]rivacy is not an optional good" because it is a "precondition for a liberal egalitarian society."[44] A legal system that enforces privacy largely through individual rights and remedies will encounter significant problems because of the difficulties for individuals to recognize the harms of relinquishing control over the information and to have the power and resources to exercise their rights.

Additionally, the traditional model's focus on privacy invasions as harms to specific individuals often overlooks the fact that certain privacy problems are structural and affect not merely particular individuals but society as a whole.[45] Privacy cannot merely be enforced at the initiative of particular individuals. Privacy, as Paul Schwartz contends, should be viewed as a "constitutive value" because "access to personal information and limits on it help form the society in which we live and shape our individual identities."[46] Since certain privacy problems are structural in nature, they affect more than specific aggrieved individuals. Social structure has effects on an entire society. As Spiros Simitis aptly observes, "privacy considerations no longer arise out of particular individual problems; rather, they express conflicts affecting everyone."[47]

B. Architecture

If we look at privacy more as an aspect of social and legal structure, then we begin to see that certain types of privacy harms are systemic and structural in nature, and we need to protect against them differently.

The concept of "architecture" is useful for understanding how certain privacy problems should be understood and dealt with. The term "architecture" typically refers to the design of spaces—of buildings or cities. I use the term "architecture" in a broader way, similar to Lawrence Lessig and Joel Reidenberg, who contend that architecture does not merely describe the design of physical structures.[48] Architecture can be constructed through computer code;

43. Anita L. Allen, *Coercing Privacy*, 40 WM. & MARY L. REV. 723 (1999).

44. *Id.* at 740.

45. Solove, *Privacy*, *supra* note 25, at 1454–55.

46. *Internet*, *supra* note 34, at 834.

47. Spiros Simitis, *Reviewing Privacy in an Information Society*, 135 U. PA. L. REV. 707, 709 (1987).

48. *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) [hereinafter *Rules*]; *see also* Joel R. Reidenberg, *Lex Informatica: The Formulation of Information Policy Rules Through Technology*, 76 TEX. L. REV. 553 (1998) [hereinafter *Lex Informatica*].

it is built into the very structure of the Internet and other forms of electronic communication, and it shapes the extent of liberty and control exercised over people in these media.[49]

Architecture emphasizes that legal and social structures are products of design. Information collection, dissemination, and networking are shaped by aspects of social and legal structure. Joel Reidenberg has long pointed out that information networks have an architecture, which is influenced not only by law but by technological considerations.[50] Architecture is an effective way to describe the way privacy is protected or diminished in our society, for the metaphor of architecture captures how legal regulations— or the lack thereof— *structure* social interaction as well as the degree of social control and freedom in a society.

Architecture does not merely structure life by direct physical limitations that channel movement (walls, distance, divisions). Architecture also alters perception by its aesthetic design, by what it expresses. Frank Lloyd Wright observed that architecture is "the scientific art of making structure express ideas."[51] Architecture creates certain psychological and social effects. As Professor Yi-Fu Tuan observes, architecture can "sharpen and enlarge consciousness."[52] "Architecture continues to exert a direct impact on the senses and feeling. The body responds, as it has always done, to such basic features of design as enclosure and exposure, verticality and horizontality, mass, volume, interior spaciousness, and light."[53]

According to Neal Katyal, physical architecture affects human conduct.[54] Architecture can structure spaces to "facilitate unplanned social interaction" by positioning door entrances so they face each other.[55] Certain architectural designs can be suffocating and constraining, such as cramped rooms and dark labyrinthine corridors. Other architectural designs can promote open space and social interaction. According to Thomas Markus, "[s]paces can be so linked that communication is free and frequent, making possible dense encounters between classes, groups, and individuals."[56]

By influencing human behavior, attitudes, thoughts, and interactions, architecture plays a profound role in the structuring of

49. *See* LESSIG, *supra* note 48.

50. *Rules, supra* note 48 at 296–99.

51. *Quoted in* John F. Nivala, *The Architecture of a Lawyer's Operation: Learning from Frank Lloyd Wright*, 20 J. LEGAL PROF. 99, 111 (1998).

52. YI-FU TUAN, SPACE AND PLACE: THE PERSPECTIVE OF EXPERIENCE 107 (1977).

53. *Id.* at 116.

54. Neal Kumar Katyal, *Architecture as Crime Control*, 111 YALE L.J. 1039 (2002).

55. *Id.* at 1064.

56. THOMAS A. MARKUS, BUILDINGS AND POWER: FREEDOM AND CONTROL IN THE ORIGIN OF MODERN BUILDING TYPES 25 (1993).

society. One of the ways in which architecture affects society is by enhancing or diminishing privacy. Architecture shapes public and private spaces. Through the use of perspectives and glass, through the positioning of rooms, doorways, and offices, physical architecture can determine what is visible or hidden.

Jeremy Bentham's design for a prison, which he called the Panopticon, demonstrates how architecture can shape the very constitution of society by affecting privacy. Bentham's design arrays prison cells around a central observation tower, from which all cells can be monitored. The prisoners, however, cannot see if there is an observer in the tower. Therefore, prisoners never know if they are actually being observed, but they know that at any moment, someone in the tower might be observing them. This fear of observation results in increased obedience and discipline in the prison. As Michel Foucault observes, "without any physical instrument other than architecture and geometry, [the Panopticon] acts directly on individuals."[57] Unlike dungeons, which served "to enclose, to deprive of light and to hide," the Panopticon achieves control through visibility.[58] The Panopticon is a form of architecture that inhibits freedom; it is an architecture of social control and discipline. For Foucault, the Panopticon is not merely consigned to physical structures such as prisons. It is an architecture that is increasingly built into the entire social system: "The panoptic schema, without disappearing as such or losing any of its properties, was destined to spread throughout the social body; its vocation was to become a generalized function."[59] As Foucault contends, we are currently within "the panoptic machine, invested by its effects of power, which we bring to ourselves since we are part of its mechanism."[60] In other words, Foucault argues that the Panopticon is the architectural design for modern power relations in society. Panoptic architecture is increasingly replicated in modern society, in both physical and non-physical forms.

Panoptic architecture, and the architecture Lessig and Reidenberg discuss, are "architectures of control,"[61] and they function to exercise greater dominion over individuals. Lessig observes that "[c]yberspace does not guarantee its own freedom but instead carries an extraordinary potential for control."[62] Architecture can function in a variety of other ways. As I will illustrate later, architecture can

57. MICHEL FOUCAULT, DISCIPLINE AND PUNISH: THE BIRTH OF THE PRISON 206 (Alan Sheridan trans., Pantheon Books 1977).

58. *Id.* at 200.

59. *Id.* at 207.

60. *Id.* at 217.

61. LESSIG, *supra* note 48, at 30.

62. *Id.* at 58.

create a world where people are vulnerable to significant harm and are helpless to do anything about it. Therefore, in addition to architectures of control, we are seeing the development of what I call "architectures of vulnerability."

If we view certain privacy problems as architectural, we begin to see how the design and structure of information flows affect movement, communication, association, and other fundamental practices in a free and democratic society. Privacy is thus an issue about the type of society we are building. Information flows are critical in shaping society in the Information Age. Our environment is not only shaped spatially by the architecture of buildings and the layout of cities, but by the design of information systems. This architecture has similar effects as spatial design on our behavior, attitudes, norms, social interaction, sense of freedom, and security.

The traditional model often views privacy problems as separate from legal structures, as social problems that are remedied by the law. We often see privacy as naturally occurring and threatened by rapidly developing technology. Law must intervene to protect privacy. However, law creates and constructs the world we live in. This is particularly true with privacy. To a significant degree, privacy is legally constructed. Law already shapes our ability to hide information and it influences information accessibility. Law makes certain information publicly available; it keeps places (such as the home) private by enforcing trespass and property laws. Law also shapes our expectations of privacy in many contexts.[63]

The law also influences much of the loss of privacy. Many privacy problems are the product of legal decisions that have been made over the past century as we have shaped our modern information economy. Once we understand the full extent of the legal construction of privacy, we will realize that privacy is not passively slipping away but is being actively eliminated by the way we are constructing the information economy through the law.

For problems that are architectural, the solutions should also be architectural. Privacy must be protected by a particular architecture, one that regulates power in our social relationships. An architecture of privacy protection is a way to structure power in social relationships between people, institutions, and the government. Unless people's relationships with bureaucracies are placed on more equal footing, affording people default property rights in information or other forms of information control will not adequately protect

63. *See* Shaun B. Spencer, *Reasonable Expectations and the Erosion of Privacy,* 39 SAN DIEGO L. REV. 843, 846–68 (2002) (discussing how courts, legislatures, and other government entities shape expectations of privacy); Solove, *supra* note 22, at 1142–43 (discussing how the law shaped expectations of privacy in postal letters).

privacy. Protecting privacy thus depends upon regulating relationships, often by enforcing limits on the power of bureaucratic organizations.

Architecture protects privacy differently than individual remedies. It is more proactive than reactive; it involves creating structures to prevent harms from arising rather than merely providing remedies when harms occur. The traditional model enforces privacy through legal remedies employed at the initiative of individuals and penalties to specific wrongdoers. Architectural remedies are more systemic in nature, and they work by altering social structure to make it harder for torts and crimes to occur. As Neal Katyal persuasively argues, architecture deals with crime differently than criminal penalties; it can prevent crime, facilitate the capture of criminals, and can even "shape individuals' attitudes toward lawbreaking."[64] Tort and criminal law often focus on individuals in ways that fail to lead to changes in architecture.

I am not contending that affording individuals a cause of action or a remedy for privacy invasions is inappropriate or completely ineffective. Indeed, individual remedies must be a component of any architecture. However, individual remedies alone are often not sufficient, for their viability and effectiveness depends upon the architecture in which they are embedded.

I am also not arguing that the traditional model is incorrect and should be abandoned. The traditional model was designed for the privacy problems experienced during the times that Warren and Brandeis wrote their article. Although it still works for a number of privacy problems today, it does not work for all privacy problems. In fact, understanding privacy problems with the notion of architecture is not in conflict with the view of privacy articulated by Warren and Brandeis. A critical part of Warren and Brandeis's argument was the importance of the law's ability to respond to new problems. Today, we face a host of different privacy problems. We need to recognize their differences and adapt the law to grapple with them rather than continue to view them through old lenses and attempt to resolve them in the same manner as other problems.

Warren and Brandeis wrote long before the rise of massive record systems and information networks. The problems created by the growing accumulation, dissemination, and networking of personal information are better understood architecturally than under the traditional model. Viewing these problems through architecture reveals that the problems are caused in a different manner than we might have originally supposed. It recognizes harm within design and

64. Katyal, *supra* note 54, at 1073–74.

structure. And it alters the strategies by which we seek to adapt law to solve the problems.

Thus far, what I have said has been relatively abstract. In the remainder of this article, I will provide a specific demonstration of these points through the example of one of the most rapidly growing and troubling problems of the information economy—the problem of identity theft.

II. Reconceptualizing Identity Theft

A. The Identity Theft Problem

A person loses his wallet while on vacation in Florida. His wallet contains his driver's license and other personal information. An identity thief uses the victim's information for more than twelve years to buy and sell property, open bank accounts, establish phone service, and so on.[65] Pursuant to a Florida warrant based on the criminal conduct of the identity thief, the victim is arrested in California and imprisoned for over a week. The victim also has civil judgments issued against him.[66]

The identity of a retired 74-year old man is stolen. Debts continue to amass on his credit reports. Although the victim lives in Maryland, a Texas bank issues a car loan to the identity thief in Texas.[67] The victim continually fights to have the debts removed from his credit reports, but he is told to take up the issues with the creditors who claim that the debts are legitimate. Even after debts are removed, they reappear on his credit reports because a different collection agency replaces them.[68]

These are examples of what has come to be called "identity theft." Identity theft is a problem involving personal information. As defined by the United States General Accounting Office, "identity theft or identity fraud generally involves 'stealing' another person's personal identifying information . . . and then using that information to fraudulently establish credit, run up debt, or take over existing financial accounts."[69] Identity theft is not the same as ordinary credit

65. U.S. GENERAL ACCOUNTING OFFICE, IDENTITY THEFT: GREATER AWARENESS AND USE OF EXISTING DATA ARE NEEDED, H.R. REP. NO. GAO-02-766, at 23 (2002) [hereinafter U.S. GAO].

66. *Id.*

67. *See* Albert B. Crenshaw, *Victims of Identity Theft Battle Creditors as Well as Crooks,* WASH. POST, July 21, 2002, at H4.

68. *Id.*

69. U.S. GAO, *supra* note 65, at 1; *see also* Jennifer 8. Lee, *Fighting Back When Someone Steals Your Name,* N.Y. TIMES, Apr. 8, 2001, at C8. For more background, see generally BETH GIVENS, THE PRIVACY RIGHTS HANDBOOK 227–48 (1997).

card fraud, where a thief steals and uses a person's credit card. In identity theft, the culprit obtains personal information and uses it in a variety of fraudulent ways to impersonate the victim. The thief obtains personal information from database companies and public records, or by stealing wallets, pilfering mail, or rooting through trash to find data on discarded documents.[70]

According to the FBI, identity theft is the most rapidly growing type of white-collar criminal activity.[71] According to estimates by the Federal Office of the Comptroller of the Currency, there are half a million victims of identity theft each year.[72] In 2001, the most common complaint of consumer fraud was identity theft,[73] constituting 42% of consumer complaints to the FTC in 2001.[74] Based on estimates, identity theft results in $5 billion in losses to financial institutions and other companies.[75]

Identity theft can be a harrowing experience, and it can be devastating to victims. According to estimates, a victim must spend over two years and close to 200 hours to repair the damage that identity theft causes.[76] Further, victims often have to spend thousands of dollars to remedy the harm.[77] Victims experience great anxiety, leading to psychological harm in certain cases.[78] Victims have difficulty "obtaining loans, mortgages, security clearances, promotions and even gaining employment."[79] And as noted above,

70. *See* Beth Givens, *Identity Theft: How It Happens, Its Impact on Victims, and Legislative Solutions,* Testimony for U.S. Senate Judiciary Committee on Technology, Terrorism, and Government Information 3–4 (July 12, 2000), *at* http://www.privacyrights.org/ar/id_theft.htm; *see also* JOHN R. VACCA, IDENTITY THEFT 8–9 (2003).

71. *See* Lee, *supra* note 69, at 8.

72. *See* O'Harrow, Jr., *supra* note 1, at A1.

73. Reuters, *Identity Theft Tops Consumer Fraud Complaints,* (Jan. 23, 2002), *at* http://www.techtv.com/news/print/0,231102,3369333,00.html.

74. *See* Yochi J. Dreazen, *U.S. Is Cracking Down on Thefts of Identity, Arresting About 130,* WALL ST. J., May 3, 2002, at B4.

75. *Id.*

76. *See* Janine Benner, Beth Givens & Ed Mierzwinski, *Nowhere to Turn: Victims Speak Out on Identity Theft,* (May 2000), *at* http://www.privacyrights.org/ar/idtheft2000.htm [hereinafter *Nowhere to Turn*]; *see also* Lee, *supra* note 69, at 8; Brandon McKelvey, *Financial Institutions' Duty of Confidentiality to Keep Customer's Personal Information Secure from the Threat of Identity Theft,* 34 U.C. DAVIS L. REV. 1077, 1086–87 (2001).

77. 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).

78. *Id.*

79. 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); *see also* Maria Ramirez-Palafox, *Identity Theft on the Rise: Will the Real John Doe Please Step Forward?,* 29 MCGEORGE L. REV. 483, 484 (1998); McKelvey, *supra* note 76, at 1087.

victims are even arrested based on warrants for the crimes of the identity thieves.[80]

Identity theft creates these problems because we are becoming a society increasingly dependent upon personal information. Our personal information dossiers are critical to our ability to function in modern life. We increasingly rely on various records and documents to assess reputation.[81] According to Steven Nock, this form of reputation, based on "credentials," enables reputations to become "portable."[82] Portability of reputation is important in modern society because people are highly mobile and creditors often lack first-hand experience of the financial condition and trustworthiness of individuals.[83] Today, creditors rely upon credit reporting agencies to obtain information about a person's credit history. The reports reveal a person's consistency in paying back debts as well as the person's loan defaulting risk. Credit reports contain a detailed financial history, financial account information, outstanding debts, bankruptcy filings, judgments, liens, and mortgage foreclosures. Today, there are three major credit reporting agencies—Equifax, Experian, and Trans Union. Each agency has compiled extensive dossiers about almost every adult United States citizen.[84] Credit reports have become essential to securing a loan, obtaining a job, purchasing a home or a car, applying for a license, or even renting an apartment.[85]

Personal information is also used to establish accounts with merchants, ISPs, cable companies, phone companies, and so on. Personal information can be employed to access various accounts and record systems with financial institutions, health organizations, schools, government agencies, and other entities.

The identity thief not only pilfers victims' personal information, but also pollutes their dossiers by adding false information, such as unpaid debts, traffic violations, parking tickets, and arrests. The harm of identity theft is not solely financial; it can permeate into a person's everyday life. The victim cannot readily recover the personal information the way stolen property can be recovered. The victim

80. Lynn M. LoPucki, *Human Identification Theory and the Identity Theft Problem*, 80 TEX. L. REV. 89, 91 (2001); *see also* Privacy Rights Clearinghouse and Identity Theft Resource Center, *Criminal Identity Theft* 89, 91 (May 2002), *at* http://www.privacyrights.org/fs/fs11g-CrimIdTheft.htm.

81. ROBERT ELLIS SMITH, BEN FRANKLIN'S WEB SITE: PRIVACY AND CURIOSITY FROM PLYMOUTH ROCK TO THE INTERNET 314 (2000).

82. STEVEN L. NOCK, THE COSTS OF PRIVACY: SURVEILLANCE AND REPUTATION IN AMERICA 3 (1993).

83. *See id.* at 3, 73.

84. For example, Experian has information on 205 million Americans. *See, e.g.*, EXPERIAN, EXPERIAN FACT SHEET, (2003), *at* http://www.experian.com/corporate/factsheet.html.

85. *See, e.g.*, VACCA, *supra* note 70, at 30.

must constantly defend against the identity thief's next move. Even after the victim cleans up her credit reports, if the identity thief remains at large, there may be further pollution. This is another way in which identity theft differs from credit card fraud or the theft of an ATM card or access card. Once the card is cancelled, the crime ends. With identity theft, the crime can continue, for personal information works like an "access card" that cannot be readily deactivated.

Additionally, the problem of identity theft is a social problem, not only a harm to particular people. Identity theft weakens the security of us all. There have been several reports of terrorists engaging in identity theft to facilitate their activities.[86] In one case, identity thieves used victims' identities to create a fake green card, Canadian passport, and Canadian citizenship card.[87] Further, beyond losses to particular individuals, identity theft results in losses to creditors, financial institutions, and companies, and these losses are passed down to consumers in the form of higher interest rates, prices, and fees.

B. Identity Theft and the Traditional Model

Thus far, identity theft has been viewed under the traditional model—as a harm to individuals by criminals. Identity theft unquestionably harms individuals and certainly involves criminals. Therefore, it is no surprise that identity theft is viewed under the traditional model and that the solutions to identity theft emerge from that model.

In 1998, Congress passed the Identity Theft and Identity Theft and Assumption Deterrence Act. The Act makes it a federal crime to "knowingly transfer or use, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law."[88] Prior to the 1998 Act, various aspects of identity theft were criminalized by a variety of other statutes at the federal level. The Act provides a more uniform and comprehensive penal regime for identity theft,[89] and it expands the means of identification constituting identity theft to include SSNs, birth dates, biometric identifiers, and other information.[90]

86. *See* Shelley Murphy & Douglas Belkin, *Terror Link Seen in Identity Thefts*, BOSTON GLOBE, Jan. 31, 2002, at A1.

87. *Id.*

88. 18 U.S.C. § 1028 (West 1998).

89. U.S. GAO, *supra* note 65, at 5.

90. *Id.*

Since 1998, the vast majority of states have passed laws to criminalize identity theft.[91] Prior to 1998, only three states had enacted identity theft statutes.[92] As of 2002, forty-four states criminalize identity theft.[93] Thus, it is only recently that policymakers have turned their attention to identity theft, and the overwhelming approach in dealing with it has been to enact criminal penalties. For example, Florida punishes identity theft as a felony, with the severity dependent upon the amount of money the thief takes,[94] and the identity thief may be required to pay restitution to the victim.[95] Likewise, New Jersey punishes identity theft based on the pecuniary amount of the injury.[96] The New Jersey statute does not provide for victims' rights and remedies. Pennsylvania has a similar scheme.[97] Arizona, one of the first states to enact an identity theft law, penalizes all identity thefts as a low-grade felony,[98] but does not address victims' rights and remedies. Unlike many other states, California, in addition to criminalizing identity theft with a maximum one year imprisonment,[99] provides assistance for victims to repair the damage. The victim can obtain the fraudulent applications made by the identity thief and a record of the transactions and charges.[100] Despite

91. *Id.* at 1.

92. *Id.* at 7.

93. *Id.* at 6.

94. Fraudulent use of personal identification information is third degree felony. FLA. STAT. ANN. § 817.568(2)(a) (2000). The offense is a second degree felony if the injury is $75,000 or more. FLA. STAT. ANN. § 817.568(2)(b) (2000). The offense is first degree misdemeanor if the personal information is used to harass the individual. FLA. STAT. ANN. § 817.568(3) (2000). If the offense was facilitated or furthered by using a public record (*see* § 119.011) the offense is reclassified to the next higher degree. FLA. STAT. ANN. § 817.568(4) (2000).

95. FLA. STAT. ANN. § 817.568(6)(a) (2000).

96. If the value received or injury is $75,000 or more the violation is a second degree crime. N.J. STAT. ANN. § 2C:21-17(c)(1) (West 2002). If the injury or value received is $500 or more but less than $75,000 the violation is a third degree crime. N.J. STAT. ANN. § 2C:21-17(c)(1) (West 2002). If the injury is $200 or more but less than $500 then the violation is fourth degree crime. N.J. STAT. ANN. § 2C:21-17(c)(1) (West 2002). If the injury is less than $200, or the person was unsuccessful in obtaining a benefit, then the violation is a disorderly persons offense. N.J. STAT. ANN. § 2C:21-17(c)(2) (West 2002).

97. Values involving less than $2000 are first degree misdemeanors. PA. STAT. ANN. tit. 18, § 4120(c)(1)(i) (West 2002). Values involving 2000 or more are third degree felonies. PA. STAT. ANN. tit. 18, § 4120(c)(1)(ii) (West 2002). The offense is a third degree felony if committed in furtherance of a criminal conspiracy regardless of the value involved. PA. STAT. ANN. tit. 18, § 4120(c)(1)(iii) (West 2002). The offense is a second degree felony regardless of the value if the offense is the third or subsequent offense. PA. STAT. ANN. tit. 18, § 4120(c)(1)(iv) (West 2002). The grading shall be one grade higher if the victim is 60 years of age or older. PA. STAT. ANN. tit. 18, § 4120(c)(2) (West 2002).

98. ARIZ. REV. STAT. ANN. § 13-2008(D)(West 2002).

99. CAL. PENAL CODE § 530.5(a) (West 2002).

100. *Id.* § 530.8(a).

some variations, these approaches view identity theft as a species of crime, akin to other forms of criminal behavior, and the law focuses on protecting people from the actions of these criminals.

There are several problems with viewing identity theft exclusively in this manner. First, law enforcement agencies have thus far not devoted adequate resources toward investigating and prosecuting identity theft cases. In a GAO survey of ten states, officials admitted that they had "insufficient" resources to respond to identity theft.[101] Resources are lacking because other crimes, such as violent crimes and drug offenses, consume significant resources.[102] Additionally, "[i]dentity theft cases require highly trained investigators, require longer-than-usual efforts, and often end without an arrest."[103] Prison sentences for identity theft are relatively short.[104] Identity theft often occurs across different jurisdictions, and law enforcement officials "sometimes tend to view identity theft as being 'someone else's problem.'"[105] As a result, most identity theft crimes remain unsolved.[106]

Second, the retrospective view of the law, which allows individuals to fix the damage caused by identity theft, is complicated by the profound lack of power individuals have over controlling their personal information. Victims experience great difficulty in obtaining redress for identity theft.

Victims are often unaware that their identities have been stolen until long after the identity theft has begun. A report based on victim surveys estimates that it takes victims over a year to discover that they have been victimized.[107] According to FTC estimates, 20% of identity theft victims learn of the theft after two years.[108] One tip-off that a person is a victim of identity theft is an unusual item on one's credit report. The identity thief often takes out loans and uses lines of credit which the thief never pays back. These delinquencies show up on the victim's credit report, and destroy the victim's credit rating. Unfortunately, the Fair Credit Reporting Act ("FCRA"),[109] which regulates credit reporting agencies, fails to provide people with adequate resources to discover that they are being victimized or repair the damage done by identity theft. Although the FCRA

101. U.S. GAO, *supra* note 65, at 17.
102. *Id.*
103. *Id.* at 18.
104. *Id.*
105. *Id.*
106. Lee, *supra* note 69, at C8.
107. *Nowhere to Turn*, *supra* note 76, at 3.
108. Jane Black, *Who's Policing the Credit Cops?*, BUS. WEEK ONLINE (Aug. 29, 2002), *at* http://www.businessweek.com/print/technology/content/aug2002/tc20020829_8532.htm.
109. 15 U.S.C. § 1681 (West 1998).

permits individuals to contest the accuracy of information in their credit histories[110] and enables individuals to sue to collect damages for violations of the Act,[111] these rights often are ineffectual. One problem is that people often do not know what information is contained in their credit reports. To obtain such information, people must pay a fee of $8.50 to each of the three major credit reporting agencies—Experian, Equifax, and Trans Union—to obtain a copy of their credit report. And individuals must do this with regularity to ensure that their credit reports remain accurate.

Credit reporting agencies have a duty to investigate consumer disputes with the accuracy of their reports, but this often is ineffective in cases of identity theft.[112] In one of the most important scholarly articles written about identity theft, Lynn LoPucki observes that the "victim is asked to prove a negative: namely, that he or she is not the person who borrowed from the creditor. The victim's evidence is likely to be complex and circumstantial."[113] Creditors do not have sufficient incentives to investigate, for if the victim is correct, creditors cannot recover on the debt.[114] LoPucki also aptly argues that the "victim lacks a forum in which to proceed. The victim has no right to a hearing on the accuracy of the information requested."[115] Moreover, the "FTC seldom acts on the complaint of a single customer."[116]

The FCRA does not allow people to sue for "defamation, invasion of privacy, or negligence" when the credit reporting agency discloses false information or a creditor reports false information to a credit reporting agency unless the information is "furnished with malice or willful intent to injure such consumer."[117] Rather, the FCRA provides a cause of action for negligently failing to comply with its provisions.[118] However, a victim must bring an action within two years "from the date on which the liability arises."[119] In *TRW, Inc. v. Andrews*,[120] the Supreme Court held that two-year statute of limitations period does not begin to run when the plaintiff discovers that the FCRA has been violated. Rather, the statute of limitations

110. *See* 15 U.S.C. § 1681i (West 1998).
111. 15 U.S.C. § 1681n (West 1998).
112. LoPucki, *supra* note 80, at 92.
113. *Id.* at 107.
114. *Id.*
115. *Id.*
116. *Id.*
117. 15 U.S.C. § 1681h(e) (West 1998).
118. 1*Id.* § 1681o.
119. *Id.* § 1681p.
120. 534 U.S. 19, 26 (2001).

begins when the violations occurred, even if the plaintiff remains unaware of the violations.

At present, the law does not allow individuals enough involvement in the uses and dissemination of their personal information to quickly discover that they are victims of identity theft or to obtain redress after identity theft occurs.

Viewing identity theft under the traditional model—as a series of isolated thefts from particular individuals—results in commentators often urging individuals to take a variety of steps to avoid being victimized. Thus, many discussions about solving identity theft include recommendations for how individuals can protect themselves against identity theft. As one commentator concludes: "[W]ith hard work, cooperation, and effective communication between law enforcement and the public, identity thieves will be held accountable."[121] Professor Fred Cate takes an even stronger position, contending that the problem of identity theft can be prevented significantly if people exercised more care over their data:

> Despite all the bills introduced to combat the theft of identity, individual action may provide the best defense: keeping a close watch on account activity; reporting suspicious or unfamiliar transactions promptly; properly destroying commercial solicitations; storing valuable documents securely; protecting account names and passwords; and never disclosing personal information to unknown callers.[122]

A report by the Federal Deposit Insurance Corporation reprinted by the FTC suggests several tips for people to "minimize" the risk of identity theft:[123]

> Pay attention to your billing cycles. . . .
>
> Guard your mail from theft . . . .
>
> Do not give out personal information . . . .
>
> Keep items with personal information in a safe place. . . .
>
> Give your SSN only when absolutely necessary. . . .
>
> Don't carry your SSN card; leave it in a secure place. . . .
>
> Order a copy of your credit report from each of the three major credit reporting agencies every year. . . .[124]

The general advice is that if people take a number of steps, identity theft will be minimized. However, personal data is often

121. Sean B. Hoar, *Identity Theft: The Crime of the New Millennium*, 80 OR. L. REV. 1423, 1447 (2001).

122. FRED H. CATE, PRIVACY IN PERSPECTIVE 22 (2001).

123. FEDERAL TRADE COMMISSION & ID THEFT: WHEN BAD THINGS HAPPEN TO YOUR GOOD NAME 3 (2002) [hereinafter FTC, BAD THINGS].

124. *Id.* at 5–7.

collected unwittingly, without consent; SSNs are frequently used and refusal to give out one's SSN results in considerable inconvenience; and many people cannot even name the three major credit reporting agencies, let alone request a copy of their credit reports, for which they are charged a fee. Even if people did take all these steps, the risks of identity theft are still not significantly minimized. According to an official at the FTC, "[t]here is no way you can fully immunize yourself from identity theft because the information is out there."[125]

I contend that the prevailing approach toward dealing with identity theft—by relying on increasing criminal penalties and by depending upon individuals to take great lengths to try to protect themselves against their vulnerabilities to identity theft—has the wrong focus. Of course, identity thieves should be prosecuted; and people should avoid being careless with their data. The law has significant room to improve in the prosecution of identity theft. But these solutions fail to address the foundations of the problem. The underlying cause of identity theft is an architecture that makes us vulnerable to such crimes and unable to adequately repair the damage.

C. Identity Theft as Architecture

Identity theft is a consequence of an architecture, one that creates a series of vulnerabilities. This architecture is not created by identity thieves; rather, it is exploited by them. It is an architecture of vulnerability, one where personal information is not protected with adequate security, where identity thieves have easy access to data and the ability to use it in detrimental ways. We are increasingly living with what I call "digital dossiers" about our lives, and these dossiers are not controlled by us but by various entities, such as private-sector companies and the government. These dossiers play a profound role in our lives in modern society. The identity thief taps into these dossiers and uses them, manipulates them, and pollutes them. The identity thief's ability to so easily access and use our personal data stems from an architecture that does not provide adequate security to our personal information and that does not afford us with a sufficient degree of participation in the collection, dissemination, and use of that information. Consequently, it is difficult for the victim to figure out what is going on and how she can remedy the situation.

The traditional view fails to address this architecture, for it focuses on identity theft as a series of discrete instances of crime rather than as a larger problem about the way our personal information is handled. Even the term of "identity theft" views it as

125. Lee, *supra* note 69, at C8.

an instance of crime—a "theft" rather than as the product of inadequate security.

The architecture enabling identity theft emerges from the government and the private sector. With regard to the government part of the structure, the Social Security number ("SSN") and public record systems create a regime where identity is readily stolen and the consequences are severe.

SSNs are a key piece of information for identity theft. SSNs can unlock a wealth of other information held by the government and the private sector.[126] The identity thief, as Lynn LoPucki observes, "ordinarily needs personal information about the victim, such as the victim's name, social security number, birth date, or mother's maiden name."[127] Thus, information enables the identity thief to apply for credit or open accounts in the victim's name.[128]

One of the primary means by which a national identification system is developing in the United States is the SSN. The SSN is currently used for identification in a number of contexts. SSNs were created in 1936 as part of the Social Security System and were not designed to be used for a general identifier. Indeed, for many years, the social security card stated that it was "NOT FOR IDENTIFICATION."[129] However, over time, numerous federal agencies began using the SSN for identification, as well as state and local governments, schools, banks, hospitals, and other private sector entities.[130]

In the early 1970s, the growing uses of the SSN raised serious concerns that the SSN would become a de facto universal identifier. In 1973, the Department of Health, Education, and Welfare issued a major report on privacy, stating:

> We take the position that a standard universal identifier (SUI) should not be established in the United States now or in the foreseeable future. By our definition, the Social Security Number (SSN) cannot fully qualify as an SUI; it only approximates one. However, there is an increasing tendency for the Social Security number to be used as if it were an SUI.[131]

126. U.S. GAO, *supra* note 65, at 7.

127. LoPucki, *supra* note 80, at 94.

128. *Id.* at 104.

129. SMITH, *supra* note 81, at 288.

130. *See, e.g.*, CHARLES J. SYKES, THE END OF PRIVACY 52 (1999); 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 (1999); SIMSON GARFINKEL, DATABASE NATION: THE DEATH OF PRIVACY IN THE 21ST CENTURY 33–34 (2000).

131. U.S. DEP'T OF HEALTH, EDUCATION, AND WELFARE, REPORT OF THE SECRETARY'S ADVISORY COMMITTEE ON AUTOMATED PERSONAL DATA SYSTEMS:

In the Privacy Act of 1974, Congress partially responded to these concerns by prohibiting government agencies from denying any right, benefit, or privilege merely because an individual refused to disclose his or her SSN. The Privacy Act was passed to "curtail the expanding use of social security numbers by federal and local agencies and, by so doing, to eliminate the threat to individual privacy and confidentiality of information posed by common numerical identifiers."[132] However, the Privacy Act did not restrict the use of SSNs by the private sector.

The use of the SSN continued to escalate after the Privacy Act.[133] SSNs are collected by private-sector database firms from a number of public and non-public sources, such as court records or credit reports. It is currently legal for private firms to sell or disclose SSNs. As one commentator has observed, "governmental dissemination of personal identifying numbers is still widespread, and limits on private actors are also virtually nonexistent."[134]

The SSN functions in the United States as a de facto identifier, and there is scant protection on its use. SSNs are often widely available. Schools frequently use student SSNs as student identifiers. This exposes student SSNs to a large number of university personnel. States often place SSNs on driver's licenses. This exposes SSNs to anybody who checks a driver's license for identification. Additionally, SSNs are requested on a wide variety of applications.

SSNs are used as passwords to obtain access to a host of personal records from banks, investment companies, schools, hospitals, doctors, and so on.[135] The SSN is a powerful number, for with it a person can open and close accounts, change addresses, obtain loans, access personal information, make financial transactions, and more. Indeed, several courts have noted the myriad ways SSNs can be misused to gain access to an individual's personal information or accounts. In *Greidinger v. Davis*,[136] the court struck down a voter registration system requiring voters to provide SSNs (which were then made publicly available). This system infringed upon the right to vote because it forced people to risk public disclosure of their SSNs

RECORDS, COMPUTERS, AND THE RIGHTS OF CITIZENS xxxii (1973) [hereinafter HEW 1973 REPORT].

132. *Doyle v. Wilson*, 529 F. Supp. 1343, 1348 (D. Del. 1982).

133. *See* U.S. GAO, *supra* note 65.

134. Flavio L. Komuves, *We've Got Your Number: An Overview of Legislation and Decisions to Control the Use of Social Security Numbers as Personal Identifiers*, 16 J. MARSHALL J. COMPUTER & INFO. L. 529, 569 (1998).

135. For example, an identity thief purchased the SSNs of several top corporate executives from Internet database companies. The thief then used the SSNs to obtain more personal information about the victims. Benjamin Weiser, *Identity Theft, and These Were Big Identities*, N.Y. TIMES, May 29, 2002, at B3.

136. 988 F.2d 1344 (4th Cir. 1993).

in order to vote, exposing them to undue risks.[137] In *Beacon Journal v. City of Akron*,[138] a court held that a state freedom of information act did not extend to public employees' SSNs:

> Thanks to the abundance of databases in the private sector that include the SSNs of persons listed in their files, an intruder using an SSN can quietly discover the intimate details of a victim's personal life without the victim ever knowing of the intrusion.[139]

According to the Court, the disclosure of SSNs would create a "high potential for fraud and victimization."[140] Likewise, in *City of Kirkland v. Sheehan*,[141] a court restricted the disclosure of law enforcement personnel's SSNs because:

> Access to an individual's SSN enables a new holder to obtain access to and to control, manipulate or alter other personal information. In effect, access to an SSN allows a person, agency or company to more efficiently and effectively search for and seize information and assets of another.[142]

In short, the SSN functions as a magic key that can unlock vast stores of records as well as financial accounts. The SSN is the identity thief's best tool.

Viewed in terms of architecture, the government has created an identification number without affording adequate precautions against its misuse. In so doing, the government has exposed every citizen to significant vulnerability to identity theft and other crimes such as fraud and stalking. Seen in this light, the problem is very much the product of the law. Identity thieves are certainly to blame, but we must also recognize the profound role that the government has played in creating the problem.

Not only are the uses of SSNs inadequately controlled, but SSNs are relatively easy for the identity thief to obtain. SSNs and other personal information that assists identity thieves can be obtained via public records or from database companies that market personal data culled from public records. Identity thieves can obtain the data to carry out their crime from various personal information record systems.[143] Public record systems can reveal a panoply of personal information, which can be aggregated and combined with other data to construct what amounts to a "digital biography" about a person.[144] There are over 165 companies that gather information from public

137. *Id.* at 1354.
138. 640 N.E.2d 164 (Ohio, 1994).
139. *Id.* at 169.
140. *Id.*
141. No. 01-2-09513-7 SEA, 2001 WL 1751590 (Wash. Super. May 10, 2001).
142. *Id.* at 2372.
143. *See* O'Harrow, Jr., *supra* note 1 at A1.
144. *See Access, supra* note 25, at 1184–95.

records across the country and peddle that data over the Internet.[145] Public records can contain SSNs, birth dates, mother's maiden names, addresses of home and work, property descriptions and value, phone numbers, photographs, height, weight, eye color, gender, email addresses, and salary information.[146] Court records can contain even more sensitive information about medical conditions, employment, and finances.[147] SSNs are in fact required by law to be publicly disclosed in bankruptcy records.[148]

Identity thieves thus can plunder public records, which are increasingly being made readily accessible on the Internet, for personal information to carry out their crimes. For example, recently the clerk of courts for Hamilton County, Ohio placed the county's public records on the Internet. From a speeding ticket placed on the website, an identity thief accessed a victim's SSN, address, birth date, signature, and other personal information and opened up credit card accounts in the victim's name.[149] Further, identity thieves can obtain SSNs and other personal information simply by paying a small fee to various database companies and obtaining a detailed dossier about their victims.[150] Some identity thieves employ information brokers and private investigators to obtain personal information, and the practices of certain information brokers and private investigators are often unsavory. One practice is hiring pretext callers, who call financial companies and impersonate a customer in order to obtain personal information.[151]

The problem, however, runs deeper than the public disclosure of SSNs and personal information. The problem stems not only from the government's creation of a de facto identifier and lax protection of it, but also from the private sector's inadequate security measures in handling personal information. Private sector entities lack adequate ways of controlling access to records and accounts in a person's name, and numerous companies engage in the common practice of using SSNs, mother's maiden names, and addresses for

145. *Id.* at 1152–53.

146. *Id.* at 1142–49.

147. *Id.* at 1145–48.

148. *See* 11 U.S.C. § 107(a) (Any "paper filed . . . and the dockets of a bankruptcy court are public records and open to examination by an entity at reasonable times without charge."); *see also* Mary Jo Obee & William C. Plouffe, Jr., *Privacy in the Federal Bankruptcy Courts,* 14 NOTRE DAME J. L. ETHICS & PUB. POL'Y 1011, 1020 (2000).

149. Jennifer 8. Lee, *Dirty Laundry Online For All to See: By Posting Court Records, Cincinnati Opens a Pandora's Box of Privacy Issues,* N.Y. TIMES, Sept. 5, 2002, at G1.

150. *See* O'Harrow, Jr., *supra* note 1, at A1.

151. Robert O'Harrow, Jr., *Three Charged With Selling Confidential Data in FTC Sting,* WASH. POST., Apr. 19, 2001, at E3.

access to account information.[152] Additionally, creditors give out credit and establish new accounts if the applicant supplies a name, SSN, and address.

The credit reporting system also employs inadequate precautions to ensure against inaccuracies in credit reports and improper access to the system. As discussed earlier, our financial reputations are currently assessed by credit reporting agencies. These companies report information about our financial condition and credit worthiness to creditors and others. People are assigned a credit score, which impacts whether they will be extended credit, and, if so, what rate of interest will be charged. Credit reporting agencies do not work for the individuals they report on; rather, they are paid by creditors. As a result, they do not establish a relationship with those they report on. Even though the FCRA gives people certain rights with regard to the information reported about them by credit reporting agencies, there is still a significant lack of accountability because credit reporting agencies have no incentive to compete for the business of those they report on. According to Lynn LoPucki, the problem emerges because "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."[153] LoPucki aptly shifts the focus away from the thieves and victims to the entities controlling personal data. He correctly contends that identity theft stems from the private sector's use of SSNs for identification.[154]

Viewed in terms of architecture, we begin to see that identity theft is part of a larger cluster of problems, caused by bureaucratization. By this, I am referring to problems emerging from the existence of information networks maintained by large bureaucratic organizations. Bureaucratic organization, Max Weber asserts, consists of a hierarchical chain-of-command, specialized offices to carry out particular functions, and a system of general rules to manage the organization.[155] Bureaucracy is not limited to public sector organizations; it is a feature of business management as well government administration.[156]

Bureaucracy is deeply ensconced in the modern world, which requires the efficient flow of information in order to communicate, to deliver goods and services, to regulate, to oversee industries, and to

152. Robert O'Harrow, Jr., *Concerns for ID Theft Often Are Unheeded,* WASH. POST, July 23, 2001, at A1; Ramirez-Palafox, *supra* note 79 at 486.

153. Lopucki, *supra* note 80, at 94.

154. *Id.* at 108–14

155. *See* MAX WEBER, ECONOMY AND SOCIETY 957–58 (Guenther Roth & Claus Wittich eds. 1978).

156. *Id.* at 974.

administer basic government functions. As Weber observes, bureaucracy is "capable of attaining the highest degree of efficiency and is in this sense formally the most rational known means of exercising authority over human beings."[157] According to Weber, bureaucracy is a superior form of organization:

> [P]recision, speed, unambiguity, knowledge of the files, continuity, discretion, unity, strict subordination, reduction of friction and of material and personal costs—these are raised to the optimum point in the strictly bureaucratic administration.[158]

Although bureaucratic organization is an essential feature of modern society and has numerous benefits, bureaucracy can also present numerous problems. As Paul Schwartz notes, bureaucracy depends upon "vast quantities of information" that "relate[] to identifiable individuals."[159] Much of this information is important and necessary to the smooth functioning of bureaucracies; but collection and use of personal data pose new dangers to privacy. As the Supreme Court noted in *Whalen v. Roe*:[160]

> The collection of taxes, the distribution of welfare and social security benefits, the supervision of public health, the direction of our Armed Forces, and the enforcement of the criminal laws all require the orderly preservation of great quantities of information, much of which is personal in character and potentially embarrassing or harmful if disclosed.[161]

There are several general tendencies of modern bureaucracies that expose people to great vulnerability. Paul Schwartz contends that because bureaucracy does not adequately protect the dignity of the people it deals with, it can "weaken an individual's capacity for critical reflection and participation in society."[162] Additionally, decisions within public and private bureaucratic organizations are often hidden from public view, decreasing accountability. As Weber notes, "[b]ureaucratic administration always tends to exclude the public, to hide its knowledge and action from criticism as well as it can."[163] Bureaucratic organizations often have hidden pockets of discretion. At lower levels, discretion can enable abuses. Frequently, bureaucracies can fail to train employees adequately and employ sub-par security measures over personal data. Bureaucracies are often careless in their uses and handling of personal information.[164]

157. *Id.* at 223.

158. *Id.* at 973.

159. Paul Schwartz, *Data Processing and Government Administration: The Failure of the American Legal Response to the Computer*, 43 HASTINGS L.J. 1321, 1332 (1992).

160. 429 U.S. 589 (1977).

161. *Id.* at 605.

162. Schwartz, *supra* note 159, at 1365.

163. WEBER, *supra* note 155, at 992.

164. Solove, *Privacy*, *supra* note 25, at 1428–29.

These bureaucratic processes exist in a world where information about people is collected, combined, and traded without their knowledge or consent. People have minimal participation in the process. They lack knowledge about what information is collected, how it is used, to whom it is disclosed, and how carefully it is protected. Privacy policies often promise that data will be kept secure, but they fail to specify how or provide enough detail for people to assess meaningfully the level of security.

Therefore, the problem runs deeper than identity theft. It is the fact that we have so little participation in our personal data combined with the fact that it flows so insecurely and carelessly without sufficient control. The harm is not simply measured in the overt instances of identity theft and abuse, but in the fact that we are made more vulnerable to a series of errors, abuses, and dangers.

With ever more frequency, we are hearing stories about security glitches and other instances of personal data being leaked and abused. For example, in one instance, explicit details of ninety psychotherapy patients' sex lives, as well as their names, addresses, telephone numbers, and credit card numbers were mistakenly posted on the Internet.[165] In 2002, identity thieves improperly used Ford Motor Credit Company's code to access the credit files of 13,000 of Ford's customers, which were maintained by Experian, a major credit reporting agency.[166] Choicepoint, a database company that gathers information about individuals and sells it to government agencies and various private sector companies, inadvertently exposed some of its databases on the Internet.[167] Citibank employed a database marketing company to collect the email addresses of its credit card customers and send them emails offering them access to their financial information.[168] This was done without verifying whether the email addresses actually belonged to the particular customers.[169]

The problems of information handling are most vividly illustrated by a recent incident involving officials at Princeton University who improperly accessed personal information maintained in a Yale University database. In December 2001, Yale University established a website enabling undergraduate applicants to find out

165. Barb Albert, *Patients' Medical Records Inadvertently Posted on Net*, INDIANAPOLIS STAR, Mar. 30, 1999, at A1.

166. Bruce Mohl, *Large-Scale Identity Theft is Painful Reminder of Risk*, BOSTON GLOBE, May 12, 2002, at C3.

167. Brian McWilliams, *Data Firm Exposes Records Online*, WIRED NEWS, (Jan. 22, 2002), *at* http://www.wired.com/news/print/0,1294,49893,00.html.

168. *See* Yochi J. Dreazen, *Citibank's E-Mail Data Offer Raises Online-Privacy Concerns*, WALL ST. J., Sept. 3, 2002, at D2.

169. *See id.*

whether they had been accepted or denied admission.[170] The website also enabled students to enter additional information, such as their interests and hobbies.[171] To gain access to the website, the students were asked their name, birth date, and SSN.[172] SSNs were chosen as a password because of their "personally identifiable nature."[173] A Princeton University admissions official accessed Yale's website and certain applicants' accounts on April 3, 2002.[174] This was made possible by the fact that these applicants had also applied to Princeton, and the Princeton admissions officials had the applicants' SSNs. After the official informed other admissions staff of the ability to log onto Yale's website, the admissions staff accessed additional student files from admissions' office computers for a total of twelve unauthorized visits to Yale's Web site.[175] Princeton officials checked certain student files more than once.[176] The Princeton official stated that he was motivated by curiosity and a desire to test the security of a Web based system because Princeton was looking into providing a similar system for admissions.[177] After discovering the unauthorized access by Princeton, Yale reported the incident to the FBI.[178]

The focus of the law in this security breach was on the actions of the Princeton officials. Yet the problem was created by Yale's inept security measures, ones that resemble in many ways those used by myriad private-sector entities that hold even more sensitive personal data and access to financial accounts.

Identity thieves exploit these inadequate security practices. Exhortations to individuals to guard their data place the onus on the wrong parties. No matter how careful people are, data is bound to leak out in some form or another. We live in an information society, and it is virtually impossible to go about daily life without giving out information to a wide variety of people and entities. Documents with sensitive personal information will be exposed in the trash. Not

170. Elise Jordan & Arielle Levin Becker, *Princeton Officials Broke Into Yale Online Admissions Decisions*, YALE DAILY NEWS, July. 25, 2002, *at* http://www.yaledailynews.com/article.asp?AID=19454; Susan Cheever, *A Tale of Ivy Rivalry Gone Awry*, NEWSDAY, July 31, 2002, at B2.

171. Jordan & Becker, *supra* note 170, at B2.

172. Tom Bell, *Princeton Punishes Hacker of Yale Site*, CHI. SUN-TIMES, Aug. 14, 2002, at 7.

173. *Id.*

174. Patrick Healy, *Princeton Says Curiosity Led To Yale Files,* BOSTON GLOBE, Aug. 14, 2002, at A2.

175. *Id.*

176. *Id.* The files of one student, Lauren Bush, the niece of President Bush, were accessed five times.

177. Kelly Heyboer, *Princeton University Decides Not to Fire Hackers*, THE STAR LEDGER, Aug. 14, 2002, at 15.

178. Cheever, *supra* note 170.

everyone will buy a shredder. Nor will all purchase "firewalls" and other computer security software. Even with additional precautions, SSNs will invariably be obtained under certain circumstances. Being secure requires individuals to take cumbersome steps, and most will never take all the necessary precautions. Even if they did, information could still be obtained by identity thieves. Much of a person's sensitive information is not exclusively in the hands of that person—it is in the hands of various companies. Some are companies that a person does business with, such as financial institutions and utility companies. But others are ones that gather data about people without their knowledge and consent. In other words, even if a person tries to keep her SSN as confidential as possible, there are many entities that have it, and its security depends upon how carefully these entities protect it. Frequently, these entities sell it to whomever is willing to pay a small fee.

The disclosure of personal information such as SSNs, birth dates, and mother's maiden names would not expose people to identity theft if this data were not used by companies as a way to verify identity. An identity thief has an easy time engaging in massive fraud given the lax security of most private sector companies.[179] For example, in one instance, an identity thief routinely found lost wallets or took discarded documents from customers at his former job. Armed with victims' SSNs, the culprit would apply for in-store instant credit at a variety of stores such as Sears, Circuit City, and Apple Computer Stores. Despite the fact that the identity thief was 47 years old, he used the identifying information of an 83-year old man, and was readily approved by a store clerk running an instant credit check.[180] As this example demonstrates, the problem emerges from the lack of care in granting credit. Banks and institutions are in a rush to grant credit, as illustrated by the fact that banks send out three billion pre-approved credit card mailings every year.[181]

Private-sector entities are not the only institutions without adequate controls on information security; government agencies are also deficient. For example, there have been instances where identity

179. One commentator aptly notes that financial institutions are partly to blame in identity theft cases because they may not keep customer data confidential, and he suggests that courts hold them liable under a theory of breach of duty of confidentiality. *See* Brandon McKelvey, *Financial Institutions' Duty of Confidentiality to Keep Personal Information Secure from the Threat of Identity Theft,* 34 U.C. DAVIS L. REV. 1077, 1122–23 (2001). Although recognizing that the problem stems from the private sector institutions, the solution still focuses on forms of individual remedies rather than architectural solutions.

180. *See* Dave Orrick, *47-Year Old Man Poses as 83-Year-Old in Financial Identity Theft Scheme,* CHI. DAILY HERALD, Aug. 16, 2002, at 1.

181. *Nowhere to Turn, supra* note 76, at 13.

thieves readily obtained driver's licenses in the names of their victims.[182]

Identity thieves, then, are only one of the culprits in identity theft. The government and private-sector entities bear a significant amount of responsibility, yet this is cloaked in the conception of identity theft as a discrete crime that the victim could have prevented had she exercised more care over her personal data. Identity theft does not merely happen; rather, it is manufactured by a legally constructed architecture.

Further, the architecture contributes to the harm caused to victims of identity theft. Identity theft plunges people into a bureaucratic nightmare. The identity theft injury to victims is often caused by the frustration and sense of helplessness in attempting to stop and repair the damage caused by the identity thief. Victims experience profound difficulty in dealing with credit reporting agencies[183] and often find recurring fraudulent entries on their credit reports even after contacting the agencies.[184] Identity theft laws do not adequately regulate the bureaucratic system that injures victims. Identity theft exposes the indifference of the bureaucracies controlling personal information to the welfare of the individuals to whom the information pertains.

The traditional model does not recognize identity theft as being constructed by the law and the under-regulated security practices of bureaucracies. Therefore, the prevailing approach continues to focus on the thieves and on how individuals can protect themselves, despite the fact that many thieves are not caught and people cannot protect themselves from identity theft. Identity theft can be prevented if we reform the architecture. It is to this issue that I now turn.

III. Forging a New Architecture

If we see the problem architecturally, we see an architecture of vulnerability, one with large holes, gaps, and weak spots. The harm is caused by the very structure itself. Living in a dilapidated structure—a building with flimsy walls, no locks, peepholes, inadequate fire protection, and no emergency exits—is harmful, even without a disaster occurring. Modern society is built on expectations—that we will be kept secure, that our money will not be stolen, that our homes will not be invaded, that we will be protected against violence. It is difficult to imagine how we could maintain a free society if we did not

182. *See* Don Oldenburg, *Identity Theft and Other Scams*, WASH. POST, Nov. 3, 1997, at D5; Bog Egelko, *Identity-theft Victim Loses DMV Suit*, SAN FRAN. CHRON., Apr. 13, 2002, at A15.

183. VACCA, *supra* note 70, at 54.

184. *Nowhere to Turn*, *supra* note 76, at 6–7.

have protection against rape, assault, murder, and theft. If these protections are inadequate, there is harm even without being victimized. People live with greater fear, they stop going places, they restrict what they do, and they alter how they live.

Effective safety is thus partly a design question. According to Neal Katyal, physical architecture can be proactive in combating crime, for it can prevent crime. For example, "cleanliness and aesthetic appeal" can make people perceive that a place is safe and orderly, and make people less likely to disrupt the place.[185] In a similar manner, the architecture of information flows can be redesigned to prevent identity theft and ameliorate its effects. Identity theft is the product of an architecture that creates vulnerability and insecurity. The most effective way to combat identity theft is to reconstruct this faulty architecture.

The recognition that identity theft is the product of architecture and is best dealt with architecturally is an important first step, for it focuses the debate on the most relevant issues and concerns. But difficult steps remain. What should an appropriate architecture that protects against identity theft look like? In the remainder of this article, I will explore architectural solutions to identity theft.

A. The Problem with Identification Systems

One of the predominant types of architectural solutions that have been proposed for resolving the problem of identity theft is the creation of a national identification system. For example, Amitai Etzioni proposes a mandatory system of national identification.[186] Etzioni advocates the use of a universal identification card that is linked to a database of personal information.[187] He recommends the use of biometric identification, which relies upon unique physical and behavioral characteristics, such as hand prints, iris and retina patterns, and facial appearance.[188] This system of identification would replace SSNs with a more reliable identifier, one that would make it harder for identity thieves to fraudulently impersonate their victims.

Although a system of national identification, if administered in a reliable manner, could curtail the problem of identity theft, it creates more problems than it will solve. Etzioni severely underestimates the dangers of creating a national identification system. As Richard Sobel observes, "[i]dentity systems and documents have a long history

185. Katyal, *supra* note 54, at 1066.
186. *See* AMITAI ETZIONI, THE LIMITS OF PRIVACY 103–37 (1999).
187. *See id.* at 113.
188. *See id.* at 115.

of uses and abuses for social control and discrimination."[189] Identification tools have been used by governments for rounding up disfavored people.[190] Etzioni contends, however, that identification systems do not "transform democratic societies into totalitarian ones. Totalitarian governments do not creep up on the trials of measures such as identification cards; they arise in response to breakdowns in the social order."[191]

Although an identification system is not necessarily a catalyst for totalitarianism, such a system is a powerful device that can be used by the government in abusive ways. For example, the Japanese-American Internment during World War II, in which over 100,000 citizens were imprisoned in camps,[192] depended upon the government's ability to identify citizens of Japanese descent.[193] Additionally, identification systems often expand beyond their initial purposes, as evidenced by the widespread expansion of the use of SSNs.[194] Beyond abuses, identification systems are far from foolproof, and one of the dangers of biometric identification is its permanent connection to the individual. A digital thumbprint, for example, can be stolen. If a password falls into the wrong hands, it can be changed; one's thumbprint cannot.[195] In short, a national identification system will pose significant dangers that may outweigh the benefits in reducing identity theft.

Lynn LoPucki recommends a different form of national identification system. LoPucki's profound contribution to the debate over identity theft is his recognition that identity theft stems from problems in identification which emerge with creditors, credit reporting agencies, and other entities using SSNs and personal data as passwords. LoPucki contends that the problem of identity theft can

189. Richard Sobel, *The Degradation of Political Identity Under a National Identification System*, 8 B.U. J. SCI. & TECH. L. 37, 48 (2002).

190. Pamela Samuelson, *Privacy as Intellectual Property?*, 52 STAN. L. REV. 1125, 1143 (2000) ("One factor that enabled the Nazis to efficiently round up, transport, and seize assets of Jews (and others they viewed as 'undesirables') was the extensive repositories of personal data available not only from the public sector but also from private sector sources.").

191. ETZIONI, *supra* note 186, at 127.

192. ERIC. K. YAMAMOTO, ET AL., RACE, RIGHTS, AND REPARATIONS: LAW AND THE JAPANESE AMERICAN INTERNMENT 39 (2001). *See also* Eugene V. Rostow, *The Japanese American Cases—A Disaster*, 54 YALE L.J. 489 (1945); Daniel J. Solove, *The Darkest Domain: Deference, Judicial Review, and the Bill of Rights*, 84 IOWA L. REV. 941 (1999).

193. WHITFIELD DIFFIE & SUSAN LANDAU, PRIVACY ON THE LINE: THE POLITICS OF WIRETAPPING AND ENCRYPTION 138 (1998); *see also* DAVID BURNHAM, THE RISE OF THE COMPUTER STATE 24 (1983).

194. *See supra* Part II.C.

195. *See* BRUCE SCHNEIER, SECRETS AND LIES: DIGITAL SECURITY IN A NETWORKED WORLD 144 (2000).

be solved by devising a better system of identification. He disfavors identity cards as a solution because they can be readily lost and forged.[196] LoPucki's proposed identification system would allow people to "publicly register their identities and publicly provide information for contacting and identifying them."[197] The system would enable people to register their identities, provide identification information, and choose from certain standard sets of instructions to potential creditors for identifying them.[198] This system would be administered by a government agency.[199] Participation would be optional.[200] The government agency would maintain the database of identification information, which would consist of various pieces of information people submit such as biometric identifying characteristics, photographs, height, drivers' license numbers, personal data, and so on.[201] LoPucki would restrict the use of SSNs as passwords, and SSNs would be publicly displayed on the website.[202] Instead of using SSNs for identification, creditors must consult the website which contains each person's instructions for how to make the identification.[203] Creditors failing to do so would "lose their statutory exemption from liability for false reporting."[204]

LoPucki's solution is clever and creative. One laudatory aspect of the system is that it allows people to participate in how they are identified.[205] The system provides people with a limited form of engagement over one aspect of their privacy—their identification.

Unfortunately, despite his great contribution toward understanding the problem of identity theft, LoPucki's solution suffers from the same problems as the traditional model. It relies too heavily upon the initiative of individuals. The system places the onus on the individual to set up an account, which requires a personal appearance. Many individuals may not be computer-savvy enough to access and monitor the website. Although it does establish a system which can assist those who decide to utilize it, LoPucki concedes that "most [people] are not likely to participate."[206] As a result, it would function as little more than a band-aid solution. Identity thieves could concentrate their efforts on the vast majority of people who do

196. LoPucki, *supra* note 80, at 110–11.
197. *Id.* at 134.
198. *See id.* at 114–35.
199. *See id.* at 115–16.
200. *See id.* at 114.
201. *See id.* at 117–18.
202. *See id.* at 119–20.
203. *See id.* at 119.
204. *Id.* at 114.
205. *See id.* at 118–19.
206. *Id.* at 114.

not participate in the system. Of course, the system could be made to be mandatory, but then it would become oppressive.

Additionally, I believe that LoPucki's solution will ultimately cause more problems than it will solve. First, it depends upon the government maintaining individuals' personal information. The government has had significant security issues with its websites in the past, and government websites have been hacked numerous times. There is no guarantee that LoPucki's government agency will have better data security practices than other government agencies.

Second, the website consisting of identifying information would be publicly accessible to all: "Read-only access to the website would be unrestricted."[207] This would widely expose this information, which could be abused in other contexts. LoPucki's focus is on creditors and credit reporting agencies, but identification can be used by a multitude of other entities for a host of other purposes. Some people do not want their address and other contact information to be publicly displayed. They may be attempting to hide from abusive spouses, stalkers, and others. LoPucki counters that people who desire to conceal their location could use only email addresses,[208] but location can still be traced. As LoPucki notes, the person must establish an email account through a national provider and must install software to detect web bugs (hidden code in emails that can obtain personal data from one's computer).[209] The requirement that people take these steps is another way in which LoPucki's system would disadvantage those who are not computer-savvy.

Third, the public disclosure of SSNs will increase the use of the number to link up records about people. Although it is certainly true that SSNs are readily obtained, the availability of SSNs in this central database will enable entities maintaining data systems to more effectively and thoroughly gather SSNs, which function to connect various personal information record systems together. As I have discussed elsewhere at length, there are significant problems with the growing aggregation of personal information by private sector entities.[210]

Furthermore, address information could be readily snatched up by database companies. LoPucki anticipates this problem and states that the website data should be "'seeded' with information that can be traced back to the website as its source."[211] An example of such seeding, LoPucki suggests, is that "the account owner might

207. *Id.* at 117.

208. *See* Lynn M. LoPucki, *Did Privacy Cause Identity Theft?*, 54 HASTINGS L.J. 1277, 1290–91 (2003) [hereinafter LoPucki II].

209. *See id.* at 1294.

210. *See generally,* Solove, *Privacy*, *supra* note 25.

211. LoPucki, *supra* note 80, at 131.

deliberately misspell words, alter capitalization, or abbreviate terms."[212] However, it is unclear whether many individuals have the sophistication to concoct creative attempts to seed their information. Even if the database were successfully seeded, this might not prevent entities from abroad from misusing the information, and these entities may be difficult to prosecute.

B. A New Architecture: Participation and Responsibility

I propose an architecture that establishes controls over the data security practices of institutions and that affords people greater participation in the uses of their information. The foundations should be formed by the Fair Information Practices, which, as Marc Rotenberg aptly observes, create an architecture for the handling and use of personal information.[213] The Fair Information Practices originate with a 1973 report by the U.S. Department of Housing, Education, and Welfare. The report recommended the passage of a code of Fair Information Practices:

> • 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.
>
> • 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.[214]

Subsequently, in 1980, the Organization for Economic Cooperation and Development ("OECD") established guidelines for the protection of privacy.[215] The OECD guidelines, building upon the HEW report, recommended eight principles: (1) collection limitation—data should be collected lawfully with the individual's consent; (2) data quality—data should be relevant to a particular

212. *Id.*

213. *See generally,* Marc Rotenberg, *What Larry Doesn't Get: Fair Information Practices and the Architecture of Privacy,* 2001 STAN. TECH. L. REV. 1 (2001).

214. HEW 1973 REPORT, *supra* note 131, at 41.

215. GUIDELINES ON THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA, *available at* http://www1.oecd.org/dsti/sti/it/secur/prod/PRIV-EN.htm. For a comparison of U.S. privacy law to the OECD guidelines, see Joel R. Reidenberg, *Restoring Americans' Privacy in Electronic Commerce,* 14 BERKELEY TECH. L.J. 771 (1999).

purpose and be accurate; (3) purpose specification—the purpose for data collection should be stated at the time of the data collection and the use of the data should be limited to this purpose; (4) use limitation—data should not be disclosed for different purposes without the consent of the individual; (5) security safeguards—data should be protected by reasonable safeguards; (6) openness principle—individuals should be informed about the practices and polices of those handling their personal information; (7) individual participation—people should be able to learn about the data that an entity possesses about them and to rectify errors or problems in that data; (8) accountability—the entities that control personal information should be held accountable for carrying out these principles.[216]

Paul Schwartz, Marc Rotenberg, Joel Reidenberg, and others have long contended that the Fair Information Practices represent the most effective foundation for the protection of privacy in the Information Age.[217] As Schwartz observes:

> A distillation of fair information principles should be made around four requirements: (1) defined obligations that limit the use of personal data; (2) transparent processing systems; (3) limited procedural and substantive rights; and (4) external oversight.[218]

The Fair Information Practices embody a particular understanding of privacy and its protection. Understood broadly, the Fair Information Practices establish an architecture that alters the power dynamic between individuals and the various bureaucracies that process their personal information. The Fair Information Practices focus on two general concerns: participation and responsibility. They aim to structure the information economy so that people can participate meaningfully in the collection and use of their personal information. This does not necessarily mean that people are afforded dominion over their personal information; rather, people are to be kept informed about the information gathered about them and the purposes of its use; and people must have some say in the way their information is processed. In other words, the Fair Information Practices aim to increase individual involvement in personal information systems.

Additionally, the Fair Information Practices bring information processing under better control. Currently, as I have discussed at

---

216. ORGANIZATION FOR ECONOMIC COOPERATION AND DEVELOPMENT, GUIDELINES ON THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA, (Feb. 2002), *available at* http://www1.oecd.org.

217. *See* Schwartz, *supra* note 159, at 1667–1703; Rotenberg, *supra* note 213, at 36–50; *see generally,* Joel R. Reidenberg, *Setting Standards for Fair Information Practice in the U.S. Private Sector,* 80 IOWA L. REV. 497 (1995).

218. Schwartz, *supra* note 159, at 1671.

great length elsewhere, information processing is out of control.[219] Companies collecting and using personal information are often doing so in careless ways with little concern for the welfare of the individuals to whom the information pertains. The Fair Information Practices recognize that personal data processors have special responsibilities and that they must be regulated in order to ensure that they maintain accurate and secure records and use and disseminate information responsibly.

The Fair Information Practices are a foundation. They are general principles, and they establish the broad goals for information privacy protection. At the most basic level, the Fair Information Practices place the burden of addressing the identity theft problem on the entities that cause it—the entities using personal information. The effectiveness of the Fair Information Practices depends upon how they are applied to particular privacy problems and how they are enforced. In what follows, I will discuss how the two general aims of the Fair Information Practices—participation and responsibility—can be implemented to help grapple with the identity theft problem.

(1) Participation

First, the architecture should allow people to have greater participation in the collection and use of their personal information. Currently, people lack knowledge about the information collected about them. Information can be readily disseminated and transferred without a person's knowledge or consent. There are few requirements for how secure information must be kept. There are rarely any limits as to whom information can be disclosed. Information can be used for whatever purpose the entity possessing it desires.

I recommend an architecture that requires entities gathering personal information about people to keep individuals informed about their information. The credit reporting system needs to be reformed. Currently, even with the FCRA, credit reporting agencies are not responsive enough to the welfare of the people whose information they collect and disseminate. For example, people should be allowed to regularly access their credit reports for free.[220] LoPucki criticizes this suggestion, contending that increasing a person's ability to access information held by credit reporting agencies will also increase the identity thief's ability to gain access as

219. *See* Solove, *Privacy*, *supra* note 25, at 1423–30.

220. In her testimony before Congress, Beth Givens recommended that "[a]ll consumers should be able to receive one free copy of their credit report annually," and noted that six states have enacted this measure into law. *See* Givens, *supra* note 70, at 6 .

well.[221] To fix this difficulty, a more radical change in the credit reporting system may be necessary. An opt-in regime to credit reporting would significantly curtail problems of improper access to credit records. Currently, credit reporting agencies need not establish any relationship to the people they report on. In an opt-in regime, credit reporting agencies would have to contact individuals and would be more accountable for improper access to credit records. Individuals could access their credit records through passwords or account numbers rather than by supplying SSNs or other personal data.

When there is an unusual change in the behavior of a record subject, such as when a person who regularly repays her loans suddenly starts defaulting, credit reporting agencies should notify that person. The architecture should empower people with an easy, quick, and convenient way to challenge inaccuracies about their personal information as well as fraudulent entries in their credit reports. Disputes can be resolved with a special arbitration system that can function quickly and inexpensively rather than resorting to expensive court proceedings.

If these measures are taken, victims will be able to discover more quickly the existence of identity theft since they will be better informed about the data collected about them and how it is being used.

(2) Responsibility

The architecture should also be premised on the notion that the collection and use of personal information is an activity that carries duties and responsibilities. The architecture would establish specific measures of control over entities maintaining systems of personal data. For example, if an entity is providing background-check information about a person, that entity should be held responsible for any inaccuracies or deficiencies in the information. After all, the information is often used to determine whether a person obtains a job, loan, or license. Currently, however, companies that collect, disseminate, and use personal information do not have many responsibilities and duties to the people to whom the information pertains.

(a) Existing Accounts and Data Holders

To establish greater responsibility, the architecture would regulate private sector security practices. For one, privacy policies often merely state that data will be kept secure and safe, but these

221. *See* LoPucki II, *supra* note 208, at 1286.

statements have little meaning without more knowledge of what practices and measures are employed. Because security is technical in nature, it is unlikely that many people will be able to understand and evaluate the specific security measures taken.

Minimum security practices must be established for handling people's personal information or accounts. An SSN, mother's maiden name, and birth date should be prohibited as the method by which access can be obtained to accounts. This is one aspect of LoPucki's solution that would be quite helpful. However, instead of establishing an elaborate voluntary public identification system as LoPucki suggests, identity theft can be curtailed by companies maintaining customer accounts employing alternative means of identification, such as passwords.

This solution does not come without difficulties. Passwords can be easily forgotten or found out. One method is the use of multiple questions and answers supplied by the customer at the time the account is created. Customers supply the question and the answer. Questions can include one's favorite songs, places a person has visited, and so on. These questions must vary from institution to institution, for standardized sets of questions will result in identity thieves attempting to find out people's answers to those questions. With varying methods of identification, an identity thief will no longer be able to use a few pieces of information to access everything. This will eliminate the severity of the impact of identity theft. The thief may be able to access one or two accounts, but not all of them. Another problem is that so much personal information is maintained by various database companies that a person's answers may exist in these databases. For example, a person might use as a password the name of her college, spouse, pet, or child. This type of information should not be used since it is readily available in databases.

Another problem that might arise is that databases will come to include the types of information that people generally use for these questions. This difficulty demonstrates the importance of thinking architecturally. The problem of identity theft is part of a larger structure in which companies are not effectively regulated in the collection, use, and dissemination of personal information. If database companies are regulated to prohibit the collection of certain types of information, then this data can be better protected from falling into the hands of an identity thief. Further, the companies maintaining accounts should use multiple series of questions rather than just one question, as this decreases the odds that the identity thief will have obtained all the necessary pieces of data.

Of course, this method of identification is far from foolproof. But the level of sophistication and difficulty needed to carry out an identity theft would be increased. Identity theft will become harder

because thieves will no longer have easy access to all accounts through the use of a few pieces of easy-to-find information such as SSNs. Additionally, identity theft can be more readily halted. It is currently a difficult and cumbersome process to change one's SSN.[222] A person cannot change her height, birth date, or mother's maiden name. But questions and answers or passwords can be easily be changed. Thus, once discovered, identity theft will be easier to stop and will not continue long after the victim becomes aware of it.

(b) New Accounts

The suggestions above concern access to already established accounts. Much identity theft, however, occurs through the identity thief opening up new accounts under the victim's identity. Currently, it is far too easy to establish a new account through the mail and the Internet.[223] Pre-approved credit card applications, for example, enable the recipient to easily establish an account and change addresses. To halt this practice, credit card companies should be required to meet with people in person when first creating the account. This will make identity thieves more reluctant to engage in fraud, as it will increase their chances of being caught. The downside to this solution is its high cost. As LoPucki also notes, it is also inconvenient for consumers.[224]

An alternative solution would be to require companies that want to open a new account through the mail to verify a person's address, date of birth, and phone number with a credit reporting agency and then send written confirmation both to the address that the applicant lists on her application as well as to the address that the credit reporting agency has. Further, the company should follow-up by calling the applicant's telephone number listed with the credit reporting agency. In the event of any discrepancies in the information held by the credit reporting agency and the individual, the individual should be notified.[225] Many attempts at identity theft can be halted if creditors take greater care at scrutinizing applications.

LoPucki contends that even with this notification system, the identity thief can still intercept the notification.[226] While this is

222. *See* Linda Foley, *Fact Sheet 17(L): Should I Change My Social Security Number?* (May 2002), *at* http://www.privacyrights.org/fs/fs171-ssn.htm.

223. Billions of pre-approved credit offers are made to consumers each year, and there is vigorous competition among creditors to find new customers. *See* Givens, *supra* note 70, at 2.

224. *See* LoPucki II, *supra* note 208, at 1285.

225. Of course, this solution would only work well if people had greater participation in the collection and use of their information by credit reporting agencies.

226. *See* LoPucki II, *supra* note 208, at 1286.

certainly possible, it requires additional steps to carry out the identity theft, ones that can increase the chances of the thief getting caught.

The solutions discussed above are only recommendations of the types of solutions that can be employed once we recognize that we need to focus on architecture. Viewing identity theft under the traditional model has diverted needed attention from these architectural concerns. If the architecture recognizes the responsibilities of companies maintaining personal data, it will provide a strong incentive for companies to devise creative solutions and better security.

(3) Foundations

These architectural solutions do not require a radical change in the law. The foundations are already present, although much remains to be built upon them. One such foundation is the Federal Trade Commission's ("FTC") enforcement over privacy policies. Beginning in 1998, the FTC began to bring actions against companies breaching their own privacy policies as a violation of the FTC Act's prohibition against "unfair or deceptive acts or practices in or affecting commerce."[227] In many of its actions thus far, the FTC has merely policed privacy policy promises. The FTC's view to enforcement has been to make practices match up to promises. As a result, the FTC has been rather weak and reactive in its enforcement of privacy policies.[228] In a number of cases involving companies engaging in blatant breaches of their own privacy policies, the FTC has settled, requiring companies simply to stop the offending practices and avoid making misrepresentations in the future.[229]

However, recently the FTC has begun to require greater security as part of its settlements. In *FTC v. Eli Lilly*,[230] a pharmaceutical company had established an email service that sent emails to patients

227. 15 U.S.C. § 45(a)(1) (2002). An unfair or deceptive act or practice is one that "causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition." 15 U.S.C. § 45(n) (2002). For a discussion of the rise of FTC privacy enforcement, see Steven Hetcher, *The FTC as Internet Privacy Norm Entrepreneur*, 53 VAND. L. REV. 2041 (2000).

228. For a discussion of FTC jurisprudence over privacy policies, see Jeff Sovern, *Protecting Privacy with Deceptive Trade Practices Legislation*, 69 FORDHAM L. REV. 1305 (2001).

229. *See, e.g.*, *In re* Liberty Financial Companies, F.T.C. No. 98-23522, (May 6, 1999) (operator of website falsely promised that personal data collected from children and teens would be kept anonymous); FTC v. ReverseAuction.com, Inc., F.T.C. No. 00-0032 (D. D.C. 2000) (company improperly obtained personal information from eBay and used it to spam eBay customers); *In re* GeoCities, F.T.C. No. C-3849 (Feb. 5, 1999) (website falsely promised that it never provided information to others without customer permission).

230. F.T.C. No. 012-3214.

reminding them to take the anti-depressant drug Prozac. Erroneously, the company sent out an email message with the email addresses of all subscribers in the "To" line. The FTC complaint alleged that Lilly failed to

> provide appropriate training for its employees regarding consumer privacy and information security; provide appropriate oversight and assistance for the employee who sent out the e-mail, who had no prior experience in creating, testing, or implementing the computer program used; and implement appropriate checks and controls on the process, such as reviewing the computer program with experienced personnel and pretesting the program internally before sending out the e-mail.[231]

The FTC appropriately focused on security issues. Eli Lilly settled and agreed to establish a new security program.[232]

Thus far, however, the FTC has been reactive, waiting for specific harms to emerge before springing to action. A recent case involving Microsoft Corporation will hopefully signal a shift toward a more proactive solution. Microsoft's .NET Passport is an online identification service that maintains personal information of Internet users (such as email addresses, gender, photographs, age, and interests) and allows users to use a single username and password to access many different websites without having to sign-on to each separately. Passport also provides a related service called Wallet that enables users to enter credit card and billing data which can then be used by multiple websites. In response to a complaint by a group of privacy organizations led by the Electronic Privacy Information Center, the FTC found on August 8, 2002, that Microsoft had violated the FTC Act, and Microsoft and the FTC agreed on a settlement.[233] Microsoft had promised in its privacy policy that it protected Passport information with "powerful online security technology," but the FTC concluded that Microsoft did not provide adequate security. As part of the settlement, Microsoft must create a "comprehensive information security program" and assess its security yearly. Further, it must make its documents about security available to the FTC for five years.

An interesting aspect of the *Microsoft Passport* case is that, unlike the *Eli Lilly* case and the other cases before the FTC, the security problems of Microsoft's Passport had not yet resulted in a major security breach. Instead of waiting for specific harms to

231. Press Release, Federal Trade Commission, *Eli Lilly Settles FTC Charges Concerning Security Breach* (Jan. 18, 2002), *at* http://www.ftc.gov/opa/2002/01/elililly.htm.

232. *See* DANIEL J. SOLOVE & MARC ROTENBERG, INFORMATION PRIVACY LAW 544–46 (2003).

233. *See In the Matter of Microsoft Corp.*, F.T.C. No. 012-3240 (2002).

emerge, the FTC acted more proactively in this case, recognizing that the harm existed in the architecture.

Unfortunately, a weakness in the proposed settlement is that the security measures do not go far enough. The consent order lacks specificity about security. Indeed, the Electronic Privacy Information Center recently commented on a number of security weaknesses that are not addressed by the consent order.[234]

Another hopeful development is the Gramm-Leach-Bliley ("GLB") Act. The GLB Act requires a number of agencies that regulate financial institutions to promulgate "administrative, technical, and physical safeguards for personal information."[235] On February 1, 2001, several agencies including the Office of the Comptroller of the Currency, the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, and the Office of Thrift Supervision issued standards for safeguarding customer information.[236] On May 23, 2002, the FTC issued similar security standards.[237] Pursuant to the FTC regulations, financial institutions "shall develop, implement, and maintain a comprehensive information security program" that is appropriate to the "size and complexity" of the institution, the "nature and scope" of the institution's activities, and the "sensitivity of any customer information at issue."[238] An information security program consists of "the administrative, technical, or physical safeguards [institutions] use to access, collect, distribute, process, store, use, transmit, dispose of, or otherwise handle customer information."[239] The regulations set forth three objectives that a security program should achieve:

> (1) Insure the security and confidentiality of customer information;
>
> (2) Protect against any anticipated threats or hazards to the security or integrity of such information; and
>
> (3) Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer.[240]

The GLB Act is on the right track in its focus on information security. The GLB Act represents an attempt at an architectural solution to the problem of information security. However, the regulations under the GLB Act remain rather vague as to the specific

234. Comments of the Electronic Privacy Information Center et al., to the Federal Trade Commission, (Sept. 9, 2002), *at* http://www.epic.org/privacy/consumer/Microsoft/ordercomments.html.

235. 15 U.S.C. § 6801(b).

236. *See* 66 Fed. Reg. 8616 (Feb. 1, 2001).

237. *See* 67 Fed. Reg. 36,484 (May 23, 2002).

238. 16 C.F.R. § 314.3(a) (2002).

239. *Id.* § 314.2(c).

240. *Id.* § 314.3(b).

level of security that is required or what types of measures should be taken. The regulations require institutions to designate personnel to "coordinate" the information security program; and to "[i]dentify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information."[241] These regulations establish rather broad obvious guidelines; they virtually ignore specifics.[242] Of course, a rule that is too detailed in the standards it required could end up being ineffective as well. As Edward Janger and Paul Schwartz observe, "command-and-control rules" which are detailed and inflexible, can "freeze development of technologies and discourage recourse to less costly alternatives."[243] Janger and Schwartz are correct that such regulations, if too specific, can quickly become obsolete, discourage innovation, and be costly and inefficient. However, rules that are too open-ended and vague can end up being toothless. Although security standards must not be overly specific, they must contain meaningful minimum requirements.

Ultimately, the strength of the GLB Act's security protections will depend upon how they are enforced. If enforced with an understanding of architecture, the GLB Act has the potential to go far in reforming security practices. However, even if the GLB Act is enforced in this manner, the Act applies only to financial institutions. A law requiring security procedures must encompass all institutions that process personal information.

Despite these new security provisions, companies continue to maintain lax security procedures for the access of financial accounts and other personal data. Thus far, the FTC's efforts have been somewhat anemic. With vigorous enforcement, security practices can change. But it remains uncertain whether the FTC and other agencies will undertake such a vigorous enforcement effort.

Conclusion

Understanding certain privacy problems as architectural—such as identity theft—demonstrates that protecting privacy involves more than protecting against isolated infractions. It is about establishing a particular social structure, one that ensures individual participation in the collection and use of personal information and responsibilities for entities that control that data. In a regime with suitable architecture, individual remedies will be far more effective. The problem of

241. 16 C.F.R. § 314.4 (2002).

242. For a good list of specific information handling practices, see Utility Consumers' Action Network & Privacy Rights Clearinghouse, *Fact Sheet 12: Responsible Information-Handling* (May 2002), *available at* http://www.privacyrights.org/fs/fs12-ih2.htm.

243. Edward J. Janger & Paul M. Schwartz, *The Gramm-Leach-Bliley Act, Information Privacy, and the Limits of Default Rules*, 86 MINN. L. REV. 1219, 1255 (2002).

identity theft may never be completely eradicated, but in a world with the appropriate architecture, its prevalence and negative effects will be significantly curtailed.