the digital person
Ex Machina: Law, Technology, and Society

General Editors: Jack M. Balkin and Beth Simone Noveck

The Digital Person
Technology and Privacy in the Information Age

Daniel J. Solove
the digital person

Technology and Privacy in the Information Age

daniel j. solove
In loving memory of
my grandma,
Jean
# Contents

Acknowledgments ix  

## 1 Introduction

The Problems of Digital Dossiers 2  
Traditional Conceptions of Privacy 7  
Rethinking Privacy 8  
A Road Map for This Book 9  

## 2 The Rise of the Digital Dossier

A History of Public-Sector Databases 13  
A History of Private-Sector Databases 16  
Cyberspace and Personal Information 22  

## 3 Kafka and Orwell:  
Reconceptualizing Information Privacy 27  

The Importance of Metaphor 27  
George Orwell's Big Brother 29
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Impact of Technology</td>
<td>131</td>
</tr>
<tr>
<td>The Regulation of Public Records</td>
<td>132</td>
</tr>
<tr>
<td>8 Access and Aggregation:</td>
<td></td>
</tr>
<tr>
<td>Rethinking Privacy and Transparency</td>
<td>140</td>
</tr>
<tr>
<td>The Tension between Transparency and Privacy</td>
<td>140</td>
</tr>
<tr>
<td>Conceptualizing Privacy and Public Records</td>
<td>143</td>
</tr>
<tr>
<td>Transparency and Privacy:</td>
<td></td>
</tr>
<tr>
<td>Reconciling the Tension</td>
<td>150</td>
</tr>
<tr>
<td>Public Records and the First Amendment</td>
<td>155</td>
</tr>
<tr>
<td>9 Government Information Gathering</td>
<td>165</td>
</tr>
<tr>
<td>Third Party Records and the Government</td>
<td>165</td>
</tr>
<tr>
<td>Government–Private-Sector Information Flows</td>
<td>168</td>
</tr>
<tr>
<td>The Orwellian Dangers</td>
<td>175</td>
</tr>
<tr>
<td>The Kafkaesque Dangers</td>
<td>177</td>
</tr>
<tr>
<td>Protecting Privacy with Architecture</td>
<td>186</td>
</tr>
<tr>
<td>10 The Fourth Amendment, Records, and Privacy</td>
<td>188</td>
</tr>
<tr>
<td>The Architecture of the Fourth Amendment</td>
<td>188</td>
</tr>
<tr>
<td>The Shifting Paradigms of Fourth Amendment Privacy</td>
<td>195</td>
</tr>
<tr>
<td>The New <em>Olmstead</em></td>
<td>200</td>
</tr>
<tr>
<td>The Emerging Statutory Regime and Its Limits</td>
<td>202</td>
</tr>
<tr>
<td>11 Reconstructing the Architecture</td>
<td>210</td>
</tr>
<tr>
<td>Scope: System of Records</td>
<td>211</td>
</tr>
<tr>
<td>Structure: Mechanisms of Oversight</td>
<td>217</td>
</tr>
<tr>
<td>Regulating Post-Collection Use of Data</td>
<td>221</td>
</tr>
<tr>
<td>Developing an Architecture</td>
<td>222</td>
</tr>
</tbody>
</table>
12 Conclusion

Notes 229
Index 267
About the Author 283
It is often said that books are written in solitude, but that wasn’t true for this one. The ideas in this book were created in conversation with many wise friends and mentors. I owe them immense gratitude. Michael Sullivan has had an enormous influence on my thinking, and he has continually challenged me to strengthen my philosophical positions. Paul Schwartz has provided countless insights, and his work is foundational for the understanding of privacy law. Both Michael’s and Paul’s comments on the manuscript have been indispensable. I also must thank Judge Guido Calabresi, Naomi Lebowitz, Judge Stanley Sporkin, and Richard Weisberg, who have had a lasting impact on the way I think about law, literature, and life.

Charlie Sullivan deserves special thanks, although he disagrees with most of what I argue in this book. He has constantly forced me to better articulate and develop my positions. I may never convince him, but this book is much stronger for making the attempt.

So many other people are deserving of special mention, and if I were to thank them all to the extent they deserve, I would more than double the length of this book. Although I only list their names, my gratitude extends much further: Anita Allen, Jack Balkin, Carl Coleman, Howard Erichson, Timothy Glynn, Rachel Godsil, Eric Goldman, Chris Hoofnagle, Ted Janger, Jerry Kang, Orin Kerr, Raymond Ku, Erik Lillquist, Michael Risinger, Marc Rotenberg, Richard St. John, Chris Slobogin, Richard Sobel, Peter Swire, Elliot Turrini, and Benno Weisberg.
I greatly benefited from the comments I received when presenting my ideas, as well as portions of the manuscript, at conferences and symposia at Berkeley Law School, Cornell University, Emory Law School, Minnesota Law School, Seton Hall Law School, Stanford Law School, and Yale Law School.

My research assistants Peter Choy, Romana Kaleem, John Spaccarotella, and Eli Weiss provided excellent assistance throughout the writing of this book. Dean Pat Hobbs and Associate Dean Kathleen Boozang of Seton Hall Law School gave me generous support.

Don Gastwirth, my agent, shepherded me through the book publishing process with great enthusiasm and acumen. With unceasing attention, constant encouragement, and superb advice, he helped me find the perfect publisher. Deborah Gershenowitz at NYU Press believed in this project from the start and provided excellent editing.

Finally, I would like to thank my parents and grandparents. Their love, encouragement, and belief in me have made all the difference.

This book incorporates and builds upon some of my previously published work: Privacy and Power: Computer Databases and Metaphors for Information Privacy, 53 Stanford Law Review 1393 (2001); Access and Aggregation: Privacy, Public Records, and the Constitution, 86 Minnesota Law Review 1137 (2002); Digital Dossiers and the Dissipation of Fourth Amendment Privacy, 75 Southern California Law Review 1083 (2002); and Identity Theft, Privacy, and the Architecture of Vulnerability, 54 Hastings Law Journal 1227 (2003). These articles are really part of a larger argument, which I am delighted that I can now present in its entirety. The articles are thoroughly revised, and parts of different articles are now intermingled with each other. The argument can now fully unfold and develop. Privacy issues continue to change at a rapid pace, and even though these articles were written not too long ago, they were in need of updating. The arguments originally made in these articles have been strengthened by many subsequent discussions about the ideas I proposed. I have been forced to think about many issues more carefully and with more nuance. My understanding of privacy is a work in progress, and it has evolved since I began writing about it. This book merely represents another resting place, not the final word.
Although information privacy law has taken some important steps to protect privacy, it has thus far suffered numerous failures and difficulties in addressing the privacy problems we are currently facing with digital dossiers. Why has such a diverse body of law failed to be effective? In a world constantly being transformed by technology, how can we erect a robust and effective law of privacy when the ground is constantly shifting?

Two Models for the Protection of Privacy

The Invasion Conception. 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.* The primary remedy for privacy invasions, they suggested, should be a tort action for damages, and to a limited extent, injunctions and criminal penalties.¹

Warren and Brandeis’s conception of privacy problems has been highly influential in the development of privacy law, and I will refer to
this understanding as the “invasion conception.” Under this conception, privacy is understood as a series of discrete wrongs—invasions—to specific individuals. These wrongs occur through the actions of particular wrongdoers. The injury is experienced by the individuals who are wronged. For example, a privacy violation that would fit well into the invasion conception is a newspaper publishing a photograph of a person in the nude without that person’s consent. 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 invasion conception, 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 invasion conception is reactive. It waits for harms to materialize in concrete form and then reacts. The invasion conception works to prevent future harms through the deterrent effects of civil liability and criminal penalties.

Another aspect of the invasion conception is that it often views privacy protections in the form of rights possessed and remedied at the initiative of the individuals whose privacy has been invaded. The value of protecting privacy is measured in terms of the value of preventing harm to the individual. In the words of one court, “[p]rivacy is inherently personal. The right to privacy recognizes the sovereignty of the individual.” 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.” Under this view, privacy is enforced by allowing individuals to seek remedies for privacy invasions.

The privacy torts are designed to redress specific harms. In many cases, however, damages are likely to be small, thus creating little 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 punishing specific wrongdoers. It aims to deter crime by establishing penalties for privacy invasions. Criminal law is often reactive, responding to crime with punishments 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 invasion conception works for a number of privacy problems, not all privacy problems are the same, and many do not fit well into this model. In particular, the invasion conception does not adequately account for many of the privacy problems arising today. The problems of digital dossiers do not consist merely of a series of isolated and discrete invasions or harms, but are systemic in nature, caused by a particular social or legal structure. Moreover, as I explained earlier, the aggregation effect complicates the application of tort law in specific cases. 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. The whole may be greater than the sum of the parts.

Further, the exchange of personal information between businesses cannot be readily analogized to the widespread disclosure of information by the media. When companies buy and sell information, they disclose it to only a few other entities. How are damages to be assessed? 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, the court of appeals struck down FCC regulations requiring that
consumers opt-in (by affirmatively giving their consent) before telecommunications carriers could use or disclose their personal information. The court reasoned that the governmental interest in protecting privacy wasn’t “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.” First Amendment scholar Eugene Volokh epitomizes this view when he writes:

[M]any of the proposals to restrict communication of consumer transactional data would apply far beyond a narrow core of highly private information, and would cover all transactional information, such as the car, house, food, or clothes one buys. I don’t deny that many people may find such speech vaguely ominous and would rather that it not take place, and I acknowledge that some people get extremely upset about it. . . . If such relatively modest offense or annoyance is enough to justify speech restrictions, then the compelling interest bar has fallen quite low.

This way of viewing the harm to privacy fails to acknowledge the larger systemic problems involved with information flow. As I have argued in chapter 3, the growing use and dissemination of personal information creates a Kafkaesque world of bureaucracy, where we 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. 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 invasion conception, 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. 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 com-
petition has interfered with private privacy protection.”7 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.”8

However, enforcement mechanisms that rely upon individual initiative often fail because individuals lack the knowledge and resources to use them. Individual remedies are only effective to the extent that individuals have power to exercise them. In the face of forces created by social structure, individual remedies are often powerless. 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. Rights to consent to the collection of data lack much meaning if people can be readily pressured, misled, or coerced into relinquishing their information.9

Additionally, the invasion conception’s focus on privacy invasions as harms to specific individuals often overlooks the fact that certain privacy problems are structural—they affect not only particular individuals but society as a whole. 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.”10 Since certain privacy problems are structural in nature, they affect more than specific aggrieved individuals. As data privacy expert Spiros Simitis aptly observes, “privacy considerations no longer arise out of particular individual problems; rather, they express conflicts affecting everyone.”11

**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, but can be constructed through computer code. 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. Both computer hardware and software have architectures. Hardware is built with certain capabilities and limitations; it only has so much memory, a limited processing speed, and so on. Likewise, software has certain constraints—some that exist because programmers have reached the range of their capabilities, but others that exist because they are created by design. The Internet itself has a design, one that affects the way people communicate, the way data is transferred, and the extent to which people can be anonymous.

Architecture creates certain psychological and social effects. According to Neal Katyal, physical architecture affects human conduct. Architecture can structure spaces to “facilitate unplanned social interaction” by positioning door entrances so they face each other. Architecture also alters perception by its aesthetic design, by what it expresses. Frank Lloyd Wright observed that architecture involves “making structure express ideas.” By influencing human behavior, attitudes, thoughts, and interactions, architecture plays a profound role in the structuring of society.

One of the ways in which architecture affects society is by enhancing or diminishing privacy. Recall from chapter 3 Jeremy Bentham’s design for a prison, the Panopticon. The Panopticon demonstrates how architecture can shape the very constitution of society by affecting privacy. Through its design with a central observation tower, the Panopticon creates a constant fear of observation, resulting in increased obedience and discipline. As Michel Foucault observes, “without any physical instrument other than architecture and geometry, [the Panopticon] acts directly on individuals.” Unlike dungeons, which served “to enclose, to deprive of light and to hide,” the Panopticon achieves control through visibility. The Panopticon is a form of architecture that inhibits freedom; it is an architecture of so-
cial 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 structure. Panoptic architecture is increasingly employed in modern society, in both physical and non-physical forms. Surveillance cameras are a prime example. Since 1994, Britain has overseen city streets through the use of about 2.5 million surveillance cameras monitored by closed circuit television (CCTV). It is virtually impossible to walk the streets of London without being captured on camera numerous times throughout the day. Such a surveillance system replicates Panoptic architecture.

Panoptic architecture, and the architecture Lessig and Reidenberg discuss, are “architectures of control,” for 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.” Lessig is responding to the early buzz about the Internet, which was hailed as a place of unprecedented freedom, a freewheeling and uninhibited world. Although the Internet certainly has the potential to be a realm of liberty, Lessig demonstrates that it can be regulated—through law and computer code. People can be traced; speech can be censored; access to information can be limited; anonymity can be restricted. Therefore, the Internet has the potential to become a realm of comprehensive control.

But beyond control, architecture can function in other problematic ways. In addition to architectures of control, we are seeing the development of what I call “architectures of vulnerability.” Architecture can create a world where people are vulnerable to significant harm and are helpless to do anything about it. Architectures of vulnerability function differently than architectures of control. Architectures of control are ways in which people are limited in their actions and their freedom, where they are pressed into conformity to another's will. In contrast, architectures of vulnerability make people weaker, expose them to a host of dangers, and take away their power. Whereas architectures of control are central to Big Brother, architectures of vulnerability pervade the world depicted by Kafka. As I will discuss later, the rapid rise in identity theft is caused by architectures of vulnerability.
For problems that are architectural, the solutions should also be architectural. Privacy must be protected by reforming the architecture, which involves restructuring our relationships with businesses and the government. In other words, the law should regulate the relationships. As I discussed earlier in this book, our relationships with businesses and the government are becoming more bureaucratic in nature, and it is this general development that must be addressed. Thus, an architectural solution goes beyond treating the troublesome symptoms that materialize from the use of digital dossiers. The law often works at the surface of the problems, dealing with the overt abuses and injuries that may arise in specific instances. But thus far the law does not do enough to redefine the underlying relationships that cause these symptoms. 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 privacy.

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 invasion conception 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.”

I am not contending that affording individuals with a cause of action or a remedy for privacy invasions is 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 invasion conception is incorrect and should be abandoned. The invasion conception was designed for the privacy problems experienced when 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 invasion conception. 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 structure. And it alters the strategies by which we seek to adapt law to solve the problems.

Thus, the viable protection of privacy must consist of more than a set of protections for a series of isolated injuries. Rather, the protection of privacy depends upon an architecture that structures power, a regulatory framework that governs how information is disseminated, collected, and networked. We need to focus on controlling power. Often, new technology is introduced without adequate controls, and as a result, it creates vulnerability and engenders troublesome shifts in power, even if the proposed uses of the technology do not seem immediately troubling and even if the threat of abuse is not imminent. The protection of privacy does not mean an all-or-nothing tradeoff between the total restriction of information gathering versus the complete absence of regulation. Many privacy problems can be ameliorated if information uses are carefully and thoughtfully controlled.

**Toward an Architecture for Privacy and the Private Sector**

What should an architecture that regulates the relationships look like? I propose an architecture that establishes controls over the data
networking practices of institutions and that affords people greater participation in the uses of their information.

The first step is to redefine the nature of our relationships to businesses and government entities that maintain and use our personal information. At present, the collectors and users of our data are often not accountable to us. A company can collect a person's data without ever contacting that person, without that person ever finding out about it. The relationship is akin to the relationship between strangers—with one very important difference: One of the strangers knows a lot about the other and often has the power to use this information to affect the other's life. But the stranger with the knowledge doesn't have many obligations to the other. At other times, we establish a relationship with a company, a bank, or another institution. We might buy a product online or open up an account and invest money. We are no longer strangers, but the quality of our relationship is often not dramatically improved. Companies collect and maintain our information; they often use it for a myriad of new purposes; and they are frequently careless about the security of our data. As discussed earlier, the law often doesn't afford people the ability to do much to change the situation.

Our relationships with the collectors and users of our personal information thus need to be redefined. Consider another set of relationships—those between us and our doctors and lawyers. Here, the law imposes a number of obligations on doctors and lawyers to focus on our welfare. Indeed, the patient-physician relationship has been likened by courts to a fiduciary one.24 A fiduciary relationship is a central facet of the law of trusts. Trustees stand in a fiduciary relationship to beneficiaries of the trust. The trustee has been entrusted with the beneficiary's money, and because of this position of special trust, the trustee owes certain special duties to the beneficiary.25 Justice Benjamin Cardozo, then writing for the Court of Appeals of New York, described fiduciary duties in a famous passage:

Many forms of conduct permissible in a workaday world for those acting at arm's length, are forbidden to those bound by fiduciary ties. A trustee is held to something stricter than the
morals of the market place. Not honesty alone, but the punctilio of an honor the most sensitive, is then the standard of behavior.26

The types of relationships that qualify as fiduciary ones are not fixed in stone. As one court has noted, courts “have carefully refrained from defining instances of fiduciary relations in such a manner that other and perhaps new cases might be excluded.”27 Examples of recognized fiduciary relationships include those between stockbrokers and clients, lawyers and clients, physicians and patients, parents and children, corporate officers and shareholders, and insurance companies and their customers.28

Fiduciaries have a duty to disclose personal interests that could affect their professional judgment as well as a duty of confidentiality.29 For example, doctors who disclose a patient’s confidential medical information have been successfully sued by patients for breach of confidentiality.30 Likewise, banks and schools have been held to be obliged to keep personal information confidential.31

I posit that the law should hold that companies collecting and using our personal information stand in a fiduciary relationship with us. This is a radical proposal. Although the concept of a fiduciary relationship is an open-ended and developing one, the concept has not been extended nearly as far as I propose. Generally, courts examine a number of factors to determine the existence of a fiduciary relationship: “[T]he degree of kinship of the parties; the disparity in age, health, and mental condition; education and business experience between the parties; and the extent to which the allegedly subservient party entrusted the handling of . . . business affairs to the other and reposed faith and confidence in [that person or entity].”32 Most of the factors look at disparities in power and knowledge, and these lean in favor of finding a fiduciary relationship between us and the collectors and users of our data. The last factor, however, understands the relationship as one in which something has been explicitly entrusted to the trustee. This will work in the context of companies that we do business with, for we entrust them with our personal data. But it will be a significant expansion of the concept of fiduciary relationships to extend it to third-party companies that gather our information
without having done business with us. We don’t entrust anything to these companies; they often take our data surreptitiously, without our consent. Nevertheless, the law is flexible and in the past has responded to new situations. The law should grow to respond here, since all of the other factors for recognizing a fiduciary relationship seem to counsel so strongly for the need to impose fiduciary obligations for the collectors and users of our personal information.

If our relationships with the collectors and users of our personal data are redefined as fiduciary ones, then this would be the start of a significant shift in the way the law understands their obligations to us. The law would require them to treat us in a different way—at a minimum, with more care and respect. By redefining relationships, the law would make a significant change to the architecture of the information economy.

More specifically, how should these relationships be reconstructed? What duties and obligations should the collectors and users of our personal information have? The foundations should be formed by the Fair Information Practices, which, as privacy expert Marc Rotenberg aptly observes, create an architecture for the handling and use of personal information. 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.
Subsequently, in 1980, the Organization for Economic Cooperation and Development (OECD) established guidelines for the protection of privacy based in large part on the Fair Information Practices. 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.

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, information processing is out of control. 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 users 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.

Unfortunately, in the United States the Fair Information Practices have only been selectively incorporated into various statutes in a limited number of contexts. A more comprehensive incorporation of the Fair Information Practices would go far toward addressing the privacy problem as I have characterized it.

**Participation: Opting-Out versus Opting-In.** The current self-regulatory and legislative solution of enabling people to opt-out of having their
data collected or disseminated is ineffectual. When people have to opt-out, the default is that they relinquish significant control over their information unless they take steps (often time-consuming and cumbersome) to indicate that they do not want a company to use or disseminate their data. Providing people with opt-out rights and privacy policies does little to give individuals much control over their information. Regulation mandating that consumers opt-in rather than opt-out will more effectively control the flow of information between unequal parties. Under a system where individuals opt-in, the default rule is that personal information cannot be collected or used about an individual unless the individual provides consent. As Jeff Sovern contends, an opt-in system will place the incentive on entities that use personal information to “make it as easy as possible for consumers to consent to the use of their personal information.” Therefore, the law should require companies to adopt an opt-in system rather than an opt-out system.

Even with an opt-in system, steps must be taken to ensure that consent amounts to more than a “notice and choice” system, which, as Marc Rotenberg argues, “imagines the creation of perfect market conditions where consumers are suddenly negotiating over a range of uses for personal information.” Thus, effective privacy regulation must legally require an opt-in system which contains a meaningful range of choices as well as addresses inequalities in knowledge and power and other impediments to voluntary and informed consent. For example, inequalities in knowledge—the fact that companies know how they might use data whereas people have little awareness of these plans—could be addressed by limiting such future uses of personal data without first obtaining people's consent.

**Limits on the Use of Data.** A critical step toward addressing the problems of digital dossiers is providing limits on the use of data. Internationally, the OECD Guidelines provide that “[p]ersonal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete, and kept up-to-date.” In 1996, the European Union issued the *European Community Directive on Data Protection*, which outlines the basic principles for privacy legislation for European Union member coun-
tries. The Directive provides for a comprehensive protection of personal information maintained by a broad range of entities. This omnibus approach exists in stark contrast to the United States’ approach, which regulates privacy “sectorally” in various narrow contexts.40

Although the Directive is far from perfect, it recognizes some of the dimensions of the problem that are neglected by U.S. privacy law. For example, Article 15 provides:

> Member States shall grant the right to every person not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc.41

Further, Article 8 prohibits, subject to a number of necessary exceptions, “the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life.”42 These two provisions of the Directive limit the ways personal information can be used to make important decisions affecting people’s lives.

Enforcement. The Fair Information Practices are broad principles, and they do not specify how they are to be carried out in practice or enforced. As I discussed earlier, individual remedies can only go so far. Of course, individual remedies are important, and people should be able to sue when injured by companies that fail to follow the Fair Information Practices. But with many of the new types of architectural harms I described—such as making people more vulnerable to fraud and identity theft—damages will be difficult to calculate. When a person actually suffers from identity theft, it is easy to comprehend the harm. When a person is made more vulnerable—such as being exposed to a greater risk of injury but not yet actually injured—it is harder to establish damages because one can’t point to concrete economic loss or physical pain and suffering. Nevertheless, increased vulnerability is a palpable harm—just as weakening a person’s
immune system would be, or disabling her home security system. Part of the challenge for law is to begin to recognize the harms created by increased vulnerability and powerlessness. But until the law does this, enforcement must also occur through the work of government agencies tasked with policing the corporate world of information networking. Just as the Food and Drug Administration (FDA) regulates food and drugs, just as the Securities and Exchange Commission (SEC) regulates the securities markets, we need a federal agency to regulate the collection and use of personal information.43 As I discussed in chapter 4, the Federal Trade Commission (FTC) has started to undertake this role, but it has a long way to go.

The FTC must receive expanded jurisdiction and resources to be more proactive in policing the security practices of companies. In a handful of cases thus far, the FTC has preemptively brought actions against companies for maintaining shoddy security even before information was leaked or obtained improperly. As discussed in chapter 4, the FTC brought an action against Microsoft for failing to provide adequate security for its users’ personal data. In In re Guess.com, Inc.,44 the FTC reached a settlement with Guess, a company that sold clothing and accessories over the Internet, for maintaining flawed security of its customers’ personal information. Guess promised that all personal information “including . . . credit card information and sign-in password, are stored in an unreadable, encrypted format at all times.” This statement was false, and the FTC brought an action even before there was any evidence that hackers or others improperly gained access to the data. Cases like these are promising developments, but many more need to be brought.

As discussed before, one problem with the FTC’s jurisdiction is that it is triggered when a company breaches its own privacy policy. But what if a company doesn’t make explicit promises about security? One 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.”45 In other words, financial institutions must adopt a security system for their data, and the minimum specifications of this system are to be defined by government agencies. A broader but similar provision must be passed to govern all
the collectors and users of personal information. It must be enforced by a federal agency that will examine each company’s security practices and ensure that they are adequate. As I will discuss later, the security practices at countless companies that collect and use our personal data are notoriously insufficient, a reality that has led to the rapid growth of identity theft.

Reconceptualizing Identity Theft

Thus far, what I have said has been relatively abstract. In the remainder of this chapter, 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. It is a privacy problem that resembles a Kafkaesque nightmare.

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 several years to buy and sell property, open bank accounts, establish phone service, and so on. 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.

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. 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.

These are examples of what has come to be called “identity theft,” which is a problem involving personal information. As defined by the U.S. 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.” Identity theft is not the same as ordinary credit 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 gathers personal information from database companies and public records, or by stealing wallets, pilfering mail, or rooting through trash to find data on discarded documents.

Identity theft is the most rapidly growing type of white-collar criminal activity. According to an FTC estimate in September 2003, “almost 10 million Americans have discovered that they were the victim of some form of ID theft within the past year.” Identity theft can be a harrowing experience. According to estimates, a victim typically spends over two years and close to 200 hours to repair the damage that identity theft causes. Victims often spend thousands of dollars to remedy the harm, and many experience great anxiety. They have difficulty getting a loan, securing a mortgage, obtaining a security clearance, or even being hired for a job. And victims are sometimes arrested based on warrants for the crimes of the identity thieves.

Identity theft creates these problems because our digital dossiers are becoming so critical to our ability to function in modern life. Credit reporting agencies construct dossiers about us to report our financial status to creditors. Without these reports, people can’t obtain loans, mortgages, or leases. Personal information is also used to establish accounts with merchants, ISPs, cable companies, phone companies, and so on.

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 seep into a person’s everyday life. The victim cannot readily recover the personal information in the way that stolen property can be recovered. The victim 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.

Identity Theft and the Invasion Conception. Thus far, the law has viewed identity theft under the invasion conception—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 invasion conception and that the solutions to identity theft emerge from this model. As I will argue later, this model is deeply flawed and as a result, its solutions are ineffective.

In 1998, Congress passed the Identity Theft and Assumption Deterrence Act, which erected a comprehensive penal regime for identity theft. Subsequently, the vast majority of states have passed laws to criminalize identity theft. Thus, it is only recently that policymakers have turned their attention to identity theft, and the overwhelming approach is to classify identity theft as a species of crime and to focus on 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 U.S. General Accounting Office survey of 10 states, officials admitted that they have insufficient resources to respond to identity theft because violent crimes and drug offenses consume most of the resources. Additionally, the survey reported, “[i]dentification theft cases require highly trained investigators, require longer-than-usual efforts, and often end without an arrest.” Identity theft often occurs across different jurisdictions, and law enforcement officials “sometimes tend to view identity theft as being ‘someone else’s problem.’” As a result, most identity thefts remain unsolved. Research firm Gartner, Inc. estimates that less than 1 in 700 instances of identity theft result in a conviction.

Second, 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. According to FTC estimates, 20 percent of identity theft victims don’t learn of the theft until
two years later. One tip-off that a person is a victim of identity theft is an unusual item on a 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), 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 permits individuals to contest the accuracy of information in their credit histories and enables individuals to sue to collect damages for violations of the Act, these rights often are ineffectual. One problem is that people often are unaware of the information their credit reports contain. To obtain such information, people must request a copy of their credit report from each of the three major credit reporting agencies—Experian, Equifax, and Trans Union. And if individuals want to ensure that their credit reports remain accurate, they must request reports regularly.

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. In a compelling article, legal scholar 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.” Creditors do not have a sufficient incentive to investigate, for if the victim is correct, creditors cannot recover on the debt. 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.” Moreover, the “FTC seldom acts on the complaint of a single customer.”

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.” Instead, the FCRA provides a cause of action for negligently failing to comply with its provisions, but a victim must bring an action within two years “from the date on which the liability arises.” In TRW, Inc. v. Andrews, the Supreme Court
held that the two-year statute of limitations period begins to run when a violation occurs, even if the plaintiff remains unaware of it.\textsuperscript{69}

In December 2003, Congress passed a law, called the Fair and Accurate Credit Transactions Act (FACTA), that revised the FCRA.\textsuperscript{70} The FACTA makes several improvements to the FCRA. It overturns Andrew\textsuperscript{71} and expands the statute of limitations to five years from the violation or two years following the discovery of the violation. A person can ask a credit reporting agency to place a “fraud alert” in her file, and the agency must contact all the other credit reporting agencies to do the same. The Act also makes it easier for identity theft victims to obtain records from companies where the thief opened accounts or purchased goods. People can request a free credit report each year from all of the national credit reporting agencies. The Act provides consumers with the ability to opt-out of offers of prescreened credit.

However, the Act is still moored in the invasion conception. 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. The FACTA makes it slightly easier for victims to repair the damage from identity theft, but this is akin to a better bandage. Many of the Act’s protections are already being carried out voluntarily by credit reporting agencies. Prior to the FACTA, victims of identity theft could call one credit reporting agency, which would voluntarily alert the others to the fraud. Most victims could already obtain a free credit report so long as they believed in good faith that they had been defrauded. Consumers who had never been victimized had to pay only $9 for their credit report. Thus, the FACTA takes some forward steps, but it does not progress very far. FACTA’s reforms are remedial; the Act does little to proactively prevent identity theft.

More disturbingly, the FACTA also gives credit reporting agencies and the companies that use our personal information a great benefit—states are barred from passing stricter laws. The states, not the federal government, had been providing stronger and more effective protection. The Act thus comes at the price of removing valuable protections to millions of individuals and preventing the states from further experimentation in combating the mounting threat of identity theft.
Viewing identity theft under the invasion conception—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. Fred Cate argues that identity theft could be greatly curtailed 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.⁷¹

A report by the FDIC suggests several tips for people to “minimize” the risk of identity theft:

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.⁷²

The general advice is that if people take a number of steps, identity theft will be minimized. However, personal data is often 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. 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.”⁷³

I contend that the prevailing approach to dealing with identity theft—by relying on criminal penalties and by depending upon individuals to take great lengths to try to protect themselves—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 prosecuting identity theft. But these solutions fail to address the foundations of the problem.

*Identity Theft as Architecture.* The underlying cause of identity theft is an architecture that makes us vulnerable to such crimes and unable to adequately repair the damage. 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 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 existence 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 its collection, dissemination, and use. Consequently, it is difficult for the victim to figure out what is going on and how to remedy the situation.

The traditional legal view of identity theft 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 “identity theft” views it as an instance of crime—a “theft” rather than 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 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, for they can unlock a wealth of other information held by the government and the private sector. Created in 1936 as part of the Social Security System, SSNs were not designed to be used as a general identifier. Indeed, for
many years, the Social Security card stated that it was “not for identification.” However, over time, numerous federal agencies began using the SSN for identification, as did state and local governments, schools, banks, hospitals, and other private-sector entities.

In the early 1970s, the growing uses of the SSN raised serious concerns that the SSN would become a de facto universal identifier. 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 her SSN. 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. As one commentator has observed, “governmental dissemination of personal identifying numbers is still widespread, and limits on private actors are also virtually nonexistent.” Today, 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, which makes student SSNs available to a large number of university personnel. States often place SSNs on driver's licenses, which exposes SSNs to anyone who checks a driver's license for identification. Additionally, SSNs are requested on a wide variety of applications and forms, such as employment applications, hospital admittance forms, college applications, video store membership applications, and credit card 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. 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. In short, the SSN functions as a magic key that can unlock vast stores of records as well as financial accounts, making it 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.
Not only are the uses of SSNs inadequately controlled, but SSNs are relatively easy for the identity thief to obtain. SSNs are harvested by 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. SSNs and other personal information that assists identity thieves can be obtained from public records or the database companies that market personal data mined from public records. SSNs are in fact required by law to be publicly disclosed in bankruptcy records. 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. Further, identity thieves can obtain SSNs along with a detailed dossier about their victims simply by paying a small fee to various database companies.

The problem of identity theft also stems from the private sector’s inadequate security measures in handling personal information. Companies 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 access to account information. 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. Credit reporting agencies don’t work for the individuals they report on; rather, they are paid by creditors. Even though the FCRA gives people certain rights with regard to 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 on whom they report. 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.” LoPucki aptly
shifts the focus to the companies that control personal data and correctly contends that identity theft stems from the private sector’s use of SSNs for identification.86

Viewed in terms of architecture, identity theft is part of a larger problem, which is best articulated by using the Kafka metaphor. The problem is that we have so little participation in the use of 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.

Indeed, with ever more frequency, we are hearing stories about security glitches and other instances of personal data being leaked and abused. For example, 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.87 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.88 This was done without verifying whether the email addresses actually belonged to the particular customers.89

The problems of information handling are most vividly illustrated by an incident involving Princeton University officials who improperly accessed personal information in a Yale University database. Yale established a website enabling undergraduate applicants to find out whether they had been accepted or denied admission.90 The website invited students to enter additional information, such as their interests and hobbies.91 To access the website, the students were asked their name, birth date, and SSN.92 However, in April 2002, a Princeton admissions official accessed certain applicants’ accounts on Yale’s website by using their SSNs.93 After discovering the unauthorized access by Princeton, Yale reported the incident to the FBI.94 Although the shady actions of the Princeton official grabbed the most attention, the problem was created by Yale’s inept security measures, ones that resemble in many ways those used by companies that hold even more sensitive personal data.

The identity thief, then, is only one of the culprits in identity theft. The government and businesses bear a significant amount of respon-
sibility, 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, and often find recurring fraudulent entries on their credit reports even after contacting the agencies. Identity theft laws do not adequately regulate the bureaucratic system that injures victims. The bureaucracies controlling personal information are often indifferent to the welfare of the individuals to whom the information pertains.

**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 architecture 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 have protection against rape, assault, murder, and theft. If these protections are inadequate, there is harm even without being victimized.

Effective safety is thus partly a design question. According to legal scholar 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 miscreants less likely to disrupt it. 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, so
the most effective way to combat identity theft is to reconstruct this faulty architecture. But what should an appropriate architecture look like?

**Participation and Responsibility.** The problem of identity theft can be addressed with an architecture built around participation and responsibility, the key concepts of the Fair Information Practices. At the most basic level, the Fair Information Practices place the burden of addressing the identity theft problem on the entities that cause it—those 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.

First, the architecture should allow for people to have greater participation in the collection and use of their personal information. Currently, information can be readily disseminated and transferred without a person's knowledge or consent. Few requirements exist for how secure information must be kept, and information can be used for whatever purpose the entity possessing it desires.

I recommend an architecture that requires companies gathering personal information about people to keep individuals informed about their information. Presently, even with the FCRA, credit reporting agencies are not responsive enough to the people whose information they collect and disseminate. The recently passed FACTA allows people to access their credit reports on a yearly basis, but identity theft can occur in the interim and can cause much damage even in a few months. People should be allowed to more regularly access their credit reports for free. But LoPucki fears 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. A more radical change in the credit reporting system may be necessary to fix this difficulty. 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 with the people on whom they report. In an opt-in regime, credit reporting
agencies would have to contact individuals and would be legally 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.

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 law should establish specific measures of control over entities maintaining systems of personal data. For example, if a company is providing background check information about a person, it should be held responsible for any inaccuracies or deficiencies in the information.

To establish greater responsibility, the law would regulate private-sector security practices. Minimum security practices must be established for handling people's personal information or accounts. Use of a SSN, mother's maiden name, and birth date as the means of gaining access to accounts should be prohibited. Identity theft can be curtailed by employing alternative means of identification, such as passwords.

This solution does not come without difficulties, as passwords can be easily forgotten or discovered. The use of multiple questions and answers supplied by the customer at the time the account is created can be effective. Questions might include favorite songs, places a person has visited, and so on, and these questions must vary from institution to institution. If varying methods of identification are used, an identity thief will no longer be able to use a few pieces of information
to access everything, which will minimize the severity of the impact of identity theft. The thief may be able to access one or two accounts, but not all of them. Unfortunately, so much personal information is already 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. Therefore, unique and less common questions and answers will provide better security against identity theft.

The possibility that databases will eventually include the types of information that people generally use for these questions 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 dissemination of certain types of information, then this data can be better protected from falling into the hands of an identity thief.

Of course, this method of identification is far from foolproof. But the level of sophistication and difficulty required to carry out an identity theft would be increased. Additionally, identity theft can be more readily halted. It is currently a difficult and cumbersome process to change one's SSN. And a person cannot change her height, birth date, or mother's maiden name. Passwords, however, can 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.

These suggestions pertain to already established accounts. Much identity theft, however, occurs through the identity thief opening up new accounts in the victim's name. Currently, it is far too easy to establish a new account through the mail and the Internet. Pre-approved credit card applications, for example, enable the recipient to easily establish an account and change addresses. Companies that want to open a new account through the mail should verify an applicant's address, date of birth, and phone number with a credit reporting agency, and then send written confirmation both to the address listed on the application and 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. 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. Many attempts at identity theft can be halted if creditors take greater care scrutinizing applications. Although the identity thief can still intercept the notification,102 it requires additional steps to carry out the identity theft, ones that can increase the chances of the thief getting caught.

The solutions just discussed 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 invasion conception has diverted 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.

Understanding certain privacy problems as architectural 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. The problem of identity theft may never be completely eradicated, but in a world with the appropriate architecture, its prevalence and negative effects will be significantly curtailed.