the digital person
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 1
   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 13
   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
Franz Kafka’s Trial 36
Beyond the Secrecy Paradigm 42
The Aggregation Effect 44
Forms of Dehumanization: Databases and the Kafka Metaphor 47

4 The Problems of Information Privacy Law 56
The Privacy Torts 57
Constitutional Law 62
Statutory Law 67
The FTC and Unfair and Deceptive Practices 72
A World of Radical Transparency: Freedom of Information Law 73
The Law of Information Privacy and Its Shortcomings 74

5 The Limits of Market-Based Solutions 76
Market-Based Solutions 76
Misgivings of the Market 81
The Value of Personal Information 87
Too Much Paternalism? 90

6 Architecture and the Protection of Privacy 93
Two Models for the Protection of Privacy 93
Toward an Architecture for Privacy and the Private Sector 101
Reconceptualizing Identity Theft 109
Forging a New Architecture 119

7 The Problem of Public Records 127
Records from Birth to Death 127
The Impact of Technology 131
The Regulation of Public Records 132

8 Access and Aggregation: Rethinking Privacy and Transparency 140
- The Tension between Transparency and Privacy 140
- Conceptualizing Privacy and Public Records 143
- Transparency and Privacy: Reconciling the Tension 150
- Public Records and the First Amendment 155

iii government access

9 Government Information Gathering 165
- Third Party Records and the Government 165
- Government–Private-Sector Information Flows 168
- The Orwellian Dangers 175
- The Kafkaesque Dangers 177
- Protecting Privacy with Architecture 186

10 The Fourth Amendment, Records, and Privacy 188
- The Architecture of the Fourth Amendment 188
- The Shifting Paradigms of Fourth Amendment Privacy 195
- The New Olmstead 200
- The Emerging Statutory Regime and Its Limits 202

11 Reconstructing the Architecture 210
- Scope: System of Records 211
- Structure: Mechanisms of Oversight 217
- Regulating Post-Collection Use of Data 221
- Developing an Architecture 222
Acknowledgments

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.
Today, much of our personal information is finding its way into the hands of third parties. Moreover, given the Court’s current conception of privacy under the Fourth Amendment, the architecture that regulates many of the government’s information gathering practices is increasingly that of a confusing and gap-riddled statutory regime.

One solution to fill the void is for the Court to reverse *Smith v. Maryland* and *United States v. Miller*. Although Fourth Amendment architecture is significantly more protective than that of the statutory regime, the problem of how to regulate government access to third party records is not adequately addressed by Fourth Amendment architecture alone. As discussed earlier, the principal remedy for Fourth Amendment violations is the exclusionary rule, which prevents the government from introducing improperly obtained data during a criminal prosecution. However, many information acquisition abuses often occur in the absence of prosecutions. Therefore, the exclusionary rule alone is not sufficiently protective.

A better architecture to regulate government information gathering from third parties should be constructed. In particular, such an
architecture should prevent the types of problems associated with government information gathering discussed earlier in chapter 9. An architecture should strive for three goals: minimization, particularization, and control.

First, government information gathering should be minimized. Sweeping investigations and vast stores of personal data in the hands of government entities present significant opportunities for the problematic uses discussed earlier.

Second, efforts at amassing data should be particularized to specific individuals suspected of criminal involvement. Particularization requires law enforcement officials to exercise care in selecting the individuals who should be investigated, and it prevents dragnet investigations that primarily involve innocent people. One of the most important aspects of keeping the government under control is to prevent its investigatory powers from being turned loose on the population at large.

Third, government information gathering and use must be controlled. There must be some meaningful form of supervision over the government’s information gathering activity to ensure that it remains minimized and particularized. The government’s use of information must be controlled to prevent abuses and security lapses.

The aims of the architecture, however, are not the most difficult issue. Substantively, the architecture needs a scope. Which information gathering activities should be regulated? Procedurally, the architecture needs a mechanism for carrying out its aims. What type of structural controls should an architecture adopt?

**Scope: System of Records**

An architecture begins with substance. It must provide guidance about which information gathering activities it governs. What is the appropriate scope of an architecture that regulates government information gathering? In particular, should the architecture cover all instances where the government gathers personal data from third parties? Restricting all information collection from third parties would prevent law enforcement officials from eliciting initial information essential to develop sufficient evidence to establish probable
cause. In the early stages of an investigation, the police frequently talk to victims, witnesses, friends, and neighbors. The police often find out about a crime when people voluntarily report suspicious activity. These examples all involve third parties who possess information about the person being investigated. If the architecture encompasses all third parties, then it might unduly constrain police investigations.

Consequently, a line must be drawn to distinguish the instances where third parties can voluntarily supply information to the government and where the government will be prohibited from accessing information. Although we may want to prevent Amazon.com from divulging to the government the log of books a person bought, we may not want to prohibit a person's neighbor or a stranger from telling the police which books she happened to observe the person reading.

Where should we draw the line? One way is to focus on the type of data involved, distinguishing between “private” and “nonprivate” information. The architecture would protect all personal information that is private. But how is privacy to be defined? Following the secrecy paradigm, the Court has defined privacy as total secrecy. But this definition obviously doesn’t work since it would exclude information held by third parties.

Another way to define private information is to focus on “intimate” information. A number of commentators, such as philosophers Julie Inness and Tom Gerety, have contended that intimacy is the essential characteristic of privacy. But what constitutes “intimate” information? Without an adequate definition, “intimate” becomes nothing more than a synonym for “private.” Some commentators, such as Inness, define “intimacy” as involving loving and caring relationships. However, much private information, such as financial and health data, doesn’t pertain to these types of relationships.

The more fundamental problem with focusing on whether information is private is that privacy is contextual and historically contingent. Easy distinctions such as intimate versus nonintimate and secret versus nonsecret fail to account for the complex nature of what is considered private. Privacy is a dimension of social practices, activities, customs, and norms that are shaped by history and culture. The matters that are considered private and public have changed throughout history. Privacy is not an inherent property of particular
forms of information, since even the most sensitive and revealing information is not private under all circumstances. Even if ordinarily a person’s sex life or medical history is private, it wouldn’t be private if that person were a public figure who routinely discussed these matters openly in public. Certainly, public disclosure does not eliminate the privacy of information; indeed, even information that is exposed to others may retain its private character. Nevertheless, privacy depends upon degrees of accessibility of information, and under certain circumstances, even highly sensitive information may not be private.

Additionally, focusing on the type of information does not solve the problem of distinguishing between the neighbor’s telling the police what books he sees a person reading and Amazon.com’s providing the police with a complete inventory of the books the person has purchased. By attempting to draw a line based upon the type of information, these two instances would be treated similarly. Another example more radically illustrates the problem. Many would deem information about a person’s genitals to be private information. Should the police be required to obtain a warrant before talking to a victim of a sexual assault about an assailant’s genitals? This would be absurd. On the other hand, many would express serious objections if the police, without probable cause, could simply compel information from the person’s doctor.

Another way a line could be drawn is based upon people’s expectations. Such an approach would draw from the Court’s notion of “reasonable expectations of privacy.” The problem with this approach, however, is that an empirical evaluation of expectations alone could gradually lead to the diminishment of privacy as more and more people come to expect that the records held by third parties can be readily obtained by the government.4

If a line cannot be drawn based upon the type of information involved or people’s expectations of privacy, then how should the line be drawn? The answer must focus on relationships. Privacy is not independent of the relationships in which it is a part. Individuals readily share information in certain private relationships, such as the family. In particular relationships people undertake certain risks, including the risk of betrayal by one with whom confidences are shared.
The fact that there are expectations and risks, however, does not mean that they must be the exclusive focus of our inquiry. The issue is not the conceivable risk of betrayal, but rather which risks people ought to assume and which risks people should be insured against. This determination has a normative dimension. When a patient discloses an ailment to a doctor, arguably the patient assumes the risk that the doctor will disclose the information to the public. However, there are several protections against this risk. Patient-physician confidentiality is protected by ethical rules, which if violated could result in the loss of the doctor's license to practice medicine. Confidentiality is also protected with an evidentiary privilege. Courts have created tort law causes of action against physicians who disclose personal information. Finally, states have passed laws that protect against the disclosure of medical information. Thus, in numerous ways, the law structures the patient-physician relationship to protect against the risk of disclosure. Similarly, the law of evidence has recognized the importance of protecting the privacy of communications between attorney and client, priest and penitent, husband and wife, and psychotherapist and patient. Our expectations in these relationships are the product of both existing norms and the norm-shaping power of the law. As Christopher Slobogin notes, “in a real sense, we only assume those risks of unregulated government intrusion that the courts tell us we have to assume.”

Therefore, the scope of the architecture should be shaped by considerations regarding social relationships. The architecture's scope should encompass all instances when third parties share personal information contained within a “system of records.” This term is taken from the Privacy Act, which defines a “system of records” as “a group of any records . . . from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.” A “system of records” is used to distinguish between collecting information by speaking with specific individuals versus obtaining it through the vast stores of records held by companies.

Focusing on systems of records targets at least two sets of relationships that must be regulated: our relationships with the government
and our relationships with the companies, employers, and other entities that possess personal information.

In relationships with the government, the focus should be on what society wants the government to be able to know rather than whether certain matters are public or private based on the extent of their exposure to others. The Court’s conception of privacy assumes that the government stands in the same shoes as everybody else, which is clearly not the case. If we allow a loved one to read our diary, do we also want the government to be able to read it? As Anthony Amsterdam has observed: “For the tenement dweller, the difference between observation by neighbors and visitors who ordinarily use the common hallways and observation by policemen who come into hallways to ‘check up’ or ‘look around’ is the difference between all the privacy that his condition allows and none.”

Indeed, the existence of Fourth Amendment protection indicates that the government stands in a different position than ordinary citizens or private-sector organizations. The possibility of aggregation and the rise of digital dossiers argue in favor of regulating the government’s access to information.

The focus should be on the goals of the architecture rather than on technical distinctions over whether information is intimate enough or secret enough. These questions should not derail attention from the important issue of whether government information gathering activities present sufficient actual and potential dangers to warrant protection. The problems discussed earlier regarding information flows from the private sector to the government stem from the extensiveness of the personal information that businesses are reaping today. Focusing on “systems of records” targets the type of information flow that raises concern. Because the problem of modern government information gathering is caused by the increasing dossiers maintained in private-sector record systems, the architecture targets those third parties that store data in record systems.

Our relationships with the entities that maintain record systems about us differ from other social relationships. Though it is possible for the government to obtain personal data by interviewing friends and others, the information in records is more permanent in nature...
and is readily aggregated. Record systems are particularly dangerous because of how easily data can be gathered, combined, stored, and analyzed.

Further, entities that maintain systems of records collect data in a power dynamic where information disclosure is often not consensual. A person can take considerable steps to prevent a stranger from collecting data without consent. For example, a person who is overzealous in gathering information can be subject to laws prohibiting stalking or harassment.

Relationships to employers and landlords, however, are different than those with our friends, neighbors, and even strangers. Currently, employers and landlords have a substantial amount of power to extort personal information. They often stand in an unequal position to that of the individual employees or tenants. The nature of the relationship with employers and landlords provides them with a significantly greater amount of power and control. If people aren’t willing to supply the information, then they may not be hired or approved as a tenant.

Relationships with merchants and communications providers might not be as directly coercive as those with the entities that govern our livelihoods and dwellings. Because these relationships are more impersonal, should it be left up to the market to decide this issue? Some might argue that if consumers demanded that companies protect their information from the government, then the market would reflect these demands.

Thus far, however, the market has not been responsive to this issue. As discussed earlier, privacy policies are often vague about information flows to the government. Individuals are usually unaware of the extent to which information about them is collected. People have difficulty bargaining over privacy, and the market fails to afford sufficient incentives to rectify this problem. Further, many companies have never established a relationship with the people whose data they have collected—and thus, there isn’t even the opportunity to bargain.

Even if people are informed, they have little choice but to hand over information to third parties. Life in the Information Age depends upon sharing information with a host of third party companies. The
Supreme Court in *Smith* and *Miller* has suggested that if people want to protect privacy, they should not share their information with third parties. However, refraining from doing so may result in people living as Information Age hermits, without credit cards, banks, Internet service, phones, and television. The market does not seem to offer a wide array of choices for people about the amount of privacy they would like to protect. As discussed in chapter 5, there is little hope that the market alone will achieve the appropriate level of protection.

Therefore, the scope of the architecture must be defined broadly to encompass any third party that maintains a “system of records.” This definition of scope is not perfect, and there may be hard cases that call for exceptions. However, this rule would provide clear guidance to law enforcement officials when gathering information from third parties. Clarity is a virtue. Unlike the existing statutory architecture, which is complicated and often full of notable gaps, this architecture has clear and simple boundaries.

**Structure: Mechanisms of Oversight**

Many different procedural mechanisms are available to control government information gathering, and they fall on a spectrum from no control to complete restriction. In the middle of the spectrum are mechanisms of oversight—where the government can access information only if it can make certain showings before a neutral and external party. This middle course will work the best.

*No Control.* On the “no control” end of the spectrum, businesses may voluntarily disclose personal information to the government. If it so desired, Amazon.com could connect its computers to the FBI’s. If a private-sector entity does not volunteer information, then the government can compel its production with a mere subpoena. The entity need not contest the subpoena or provide notice to the person to whom the information pertains. Whether the entity does so would be left up to market forces—to contracts between the entity and the consumer or privacy policies. The problem with “no control” is that it does nothing to solve the problems caused by government information gathering.
Mechanisms of Restriction. On the other end of the spectrum are architectural mechanisms of restriction—prohibitions on government collection and use of information. These mechanisms are embodied in the architecture of the Fifth Amendment. The Fifth Amendment provides that “[n]o person . . . shall be compelled in any criminal case to be a witness against himself.” The Fifth Amendment’s privilege against self-incrimination prevents the government from compelling individuals to testify against themselves, and completely bars use of the information obtained in violation of the right at trial. In contrast, under current Fourth Amendment architecture, evidence is admissible at trial so long as the government obtains it with a valid search warrant.

At one point in its history, the Fourth Amendment used to rely heavily on mechanisms of restriction. Early cases, such as Boyd v. United States, and Gouled v. United States, held that the government could seize a person’s private papers only if they were instrumentalities of a crime—in other words, only if they were actually used to commit the crime. If they were merely evidence of a crime, however, the government couldn’t obtain them—even with a warrant. This rule became known as the “mere evidence” rule. The Court later overturned it.

Perhaps the mere evidence rule should be resurrected and applied to third party records. This would effectively bar the government from obtaining the records. The problem with this solution is that it would cripple modern criminal investigation. As William Stuntz observes: “Government regulation require[s] lots of information, and Boyd came dangerously close to giving regulated actors a blanket entitlement to nondisclosure. It is hard to see how modern health, safety, environmental, or economic regulation would be possible in such a regime.” Because Boyd rested in part on the Fifth Amendment, it completely prevented the government from obtaining and using the papers against the defendant no matter what procedure the government had used to obtain them. This approach is far too restrictive when it comes to most personal information maintained in third party records.

Mechanisms of Oversight. In the middle of the spectrum are mechanisms of oversight. An architecture containing this type of mecha-
nism is preferable to regulate government access of records held by third parties maintaining “systems of records.” Mechanisms of oversight allow the government to gather information, but the government must first justify its need to do so by presenting facts and evidence before a neutral detached judge or magistrate. Oversight is embodied in the Fourth Amendment’s per se warrant rule. The warrant requirement achieves the aims of minimization, particularization, and control. Collection is minimized by the requirement that the government justify that its information gathering is legitimate and necessary. The warrant ensures particularization with its requirement that there be probable cause that a particular person be engaged in criminal activity or that particular place contains evidence of a crime. Finally, the warrant achieves control (at least over the collection efforts) by having a neutral and detached party authorize the collection.

In many cases, warrants are the best regulatory device for government information gathering. Often, at the point during an investigation when certain information from third parties becomes important to obtain, there is already enough evidence to support a warrant. In both Smith and Miller there was probably sufficient evidence for the police to secure warrants. Therefore, the requirement of a warrant prevents cases of illegitimate abuses—such as large-scale information sweeps and investigations without particularized suspicion—without unduly interfering with legitimate law enforcement activities. Further, third party records have few of the dangers that make warrants inefficient. For example, because third parties maintain the records, there are fewer opportunities for a suspect to hide or destroy documents during the time law enforcement officials obtain a warrant.

However, as discussed previously, merely applying the Fourth Amendment to government access to third party records proves inadequate. The exclusionary rule only provides a remedy at trial, and many of the abuses associated with government information gathering extend far beyond criminal trials. Therefore, I recommend a fusion between warrants and subpoenas.

Despite being far more permissive for government information collection purposes, subpoenas have certain protections not available
with search warrants. Unlike warrants, they can be challenged prior to the seizure of the documents. The subpoenaed party can refuse to comply and make a motion to quash before a judge. Further, subpoenas permit the target to produce the documents rather than have government agents rummage through a person’s home or belongings. The advantages of subpoenas over search warrants are best illustrated in *Zurcher v. The Stanford Daily*, where the police searched a newspaper’s offices for evidence relating to a criminal suspect. The newspaper was not involved in the alleged crime; it merely possessed evidence. The Court upheld the search because the police obtained a valid warrant. Dissenting justices contended that there were First Amendment concerns with searches of newspaper offices because they would disrupt journalistic activities and result in “the possibility of disclosure of information received from confidential sources, or of the identity of the sources themselves.” Congress responded to *Zurcher* by passing the Privacy Protection Act of 1980, which restricts the use of search warrants for offices of newspapers and other media entities for evidence of crimes of other parties. In effect, the Act requires the use of subpoenas in addition to warrants to obtain such evidence.

The benefits of subpoenas, however, often do not apply when they are issued on the third parties to produce an individual’s records. The third party does not need to notify the individual or may not have any incentive to challenge the subpoena in court. Further, as discussed earlier, subpoenas have many weaknesses compared to warrants, such as a lack of requiring particularized suspicion and little protection by way of oversight by the judiciary.

Therefore, the Fourth Amendment architecture should be resurrected statutorily, by creating a requirement that the government obtain a special court order—a fusion between a warrant and a subpoena. From warrants, the standard of probable cause should be used. This threshold would require government officials to go before a judge with specific facts and evidence that a particular person is involved in criminal activity. For example, a probable cause standard would prevent government officials from scouring through databases to locate all people who bought books about bomb making or drug manufacturing. Such a search is akin to the types of general searches
that the Framers wanted to forbid. From subpoenas, advance notice should be provided to the person whose records are involved, and that person should be able to challenge the order in court. This statutory regime would incorporate the exclusionary rule, a minimum statutory damages provision, and a framework for disciplining offending law enforcement officials.

Moreover, third parties maintaining personal information in a “system of records” should be restricted from voluntarily disclosing an individual’s personal information to the government except under special circumstances. Exceptions might include allowing disclosure to prevent an imminent threat of harm to another. Another exception would allow the individual to whom the records pertain to authorize the government to obtain them from the third party. For example, if a victim of computer hacking wanted to permit the government to access the victim’s own ISP records, the victim could authorize the government to do so.

Regulating Post-Collection Use of Data

Another problem that must be addressed is the way personal information is used once it has been collected. As Stuntz astutely observes: “Fourth Amendment law regulates the government’s efforts to uncover information, but it says nothing about what the government may do with the information it uncovers. Yet as the Clinton investigation shows, often the greater privacy intrusion is not the initial disclosure but the leaks that follow.” Legal scholar Carol Steiker notes: “Unlike other countries in North America and Western Europe, the United States [has] never developed a national plan to organize a ‘system’ of policing or to provide for centralized control over police authority.” Once information is collected, the Fourth Amendment’s architecture of oversight no longer applies. This is problematic, as many of the abuses of information by the government occur after the information has been collected.

The Privacy Act of 1974 provides some limited regulation of records maintained by law enforcement entities. But as discussed earlier in chapter 8, the Act contains many exceptions and loopholes that have limited its effectiveness. Government entities often can share
information widely with each other.\textsuperscript{26} Additionally, the Act applies only to the federal government.

The Privacy Act is an important first step in reining in the vast stores of data that government entities collect. There remains, however, much room for the Privacy Act to be improved and strengthened. One possible safeguard is to mandate the destruction of data after a certain period of time or, mandate the transfer of data to the judicial branch after a certain period of time for access only under special circumstances. Another way is to adopt a meaningful purpose specification restriction. This means that, with certain reasonable exceptions, information collected from third party records may only be used for the particular purpose for which it is collected.

\textbf{Developing an Architecture}

The government’s increasing access to our digital dossiers is one of the most significant threats to privacy of our times, and it is inadequately regulated. The Court’s Fourth Amendment jurisprudence has been mired in the difficulties of conceptualizing privacy, thus preventing the application of the Fourth Amendment. A statutory regime has arisen to fill the void, but it is severely flawed. A new architecture must be constructed, one that effectively regulates the government’s collection and use of third party records. The process toward developing an appropriate architecture should begin by regulating both the government’s acquisition of personal data and its downstream uses of it. As for acquiring personal information stored in a system of records, the government should be required to obtain a special court order that combines the benefits of subpoenas and warrants. As for downstream uses, specific limits must be established for how long the government can keep personal information and for what the government can do with it. The task of developing an architecture is not easy in a rapidly changing society that is adjusting to the new dimensions of the Information Age. This proposed solution is thus a beginning of the process.