the digital person
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 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: 27
   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

ii public records

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

8 Access and Aggregation:
Rethinking Privacy and Transparency
The Tension between Transparency and Privacy
Conceptualizing Privacy and Public Records
Transparency and Privacy:
Reconciling the Tension
Public Records and the First Amendment

iii government access

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

10 The Fourth Amendment, Records, and Privacy
The Architecture of the Fourth Amendment
The Shifting Paradigms of
Fourth Amendment Privacy
The New *Olmstead*
The Emerging Statutory Regime and Its Limits

11 Reconstructing the Architecture
Scope: System of Records
Structure: Mechanisms of Oversight
Regulating Post-Collection Use of Data
Developing an Architecture
## 12 Conclusion

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Notes</td>
<td>229</td>
</tr>
<tr>
<td>Index</td>
<td>267</td>
</tr>
<tr>
<td>About the Author</td>
<td>283</td>
</tr>
</tbody>
</table>
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.
The Tension between Transparency and Privacy

A 1998 episode of the television newsmagazine Dateline illustrates one way that the tension between transparency (open access to public records) and privacy can arise. A man, imprisoned for murder, obtained under a state FOIA the address of a former girlfriend. When she learned that her ex-boyfriend obtained her address, the woman became quite scared because her ex-boyfriend was prone to losing his temper and held a grudge against her. She lived in fear, knowing that someday he would be released and might come after her. The prisoner, however, claimed that he was the father of her child and needed the address because he wanted to file a paternity suit. This story illustrates why it is important for people to be able to obtain certain information about others, yet also demonstrates the dangers and threat to privacy caused by the ready availability of information.

There are at least four general functions of transparency: (1) to shed light on governmental activities and proceedings; (2) to find out information about public officials and candidates for public office; (3) to facilitate certain social transactions, such as selling property or initiating lawsuits; and (4) to find out information about other individuals for a variety of purposes.
First, and perhaps most importantly, transparency provides the public with knowledge about the government and an understanding of how it functions. By promoting awareness of the workings of government, transparency serves a “watchdog” function. Open access to government proceedings ensures that they are conducted fairly. Open access exposes the government to public scrutiny and enables a check on abuse and corruption. “Sunlight is said to be the best of disinfectants,” declared Justice Brandeis, “electric light the most efficient policeman.”

Making arrest records public, for example, protects against secret arrests and government abuses. Open access to public court records “allows the citizenry to monitor the functioning of our courts, thereby insuring quality, honesty, and respect for our legal system.” As James Madison observed: “A popular Government, without popular information, or the means of acquiring it, is but a Prologue to a Farce or a Tragedy; or, perhaps both. Knowledge will forever govern ignorance: And a people who mean to be their own Governors, must arm themselves with the power which knowledge gives.”

According to Justice Oliver Wendell Holmes:

> It is desirable that the trial of [civil] causes should take place under the public eye not because the controversies of one citizen with another are of public concern, but because it is of the highest moment that those who administer justice should always act under the sense of public responsibility, and that every citizen should be able to satisfy himself with his own eyes as to the mode in which a public duty is performed.

Access to court records permits people to examine the information considered by courts making decisions affecting the public at large. Issues raised in a product liability case could have significance for millions of others who use a product. Information about how certain types of cases are resolved—such as domestic abuse cases, medical malpractice cases, and others—is important for assessing the competency of the judicial system for resolving important social matters. Scholars and the media need to look beyond a judicial decision or a jury verdict to scrutinize the records and evidence in a case. The ability to identify jurors enables the media to question them about the reasons for their verdict. Courts and commentators have pointed out
that the Watergate Scandal might never have been uncovered if the original bail hearing had been closed to the press because reporters Bob Woodward and Carl Bernstein would not have been suspicious that expensive attorneys were representing the burglars.7

The second function of transparency is to enable the scrutiny of public officials or candidates for public office. Information about a politician's criminal history might be informative to many voters. Information about a politician's property may provide insight into the politician's wealth, a factor that might shape the politician's values and public decisions. Some voters may find a politician's divorce records and marital history illustrative of the person's character. Other possibly informative information about a politician could include that she was sued many times or sued others many times; that she once declared bankruptcy; that she never voted in any elections; that she was formerly registered in another political party; that she owns property in other states; and so on. Open access to public records enables voters to find out such information so they may make more informed choices at the polls.

Third, transparency facilitates certain social transactions. Access to public records is an essential function for the sale and transfer of property, as it enables people to trace ownership and title in land. Public record information is useful in locating witnesses for judicial proceedings as well as locating heirs to estates. Further, access to public records can allow individuals and entities to track down individuals they want to sue and to obtain the necessary information to serve them with process.

The fourth function of transparency is to enable people to find out information about individuals for various other purposes. Public records can help verify individual identity, investigate fraud, and locate lost friends and classmates. Public records enable law enforcement officials to locate criminals and investigate crimes, and can assist in tracking down deadbeat parents. Public records can permit people to investigate babysitters or child care professionals. Employers can use public record information to screen potential employees, such as examining the past driving records of prospective truck drivers or taxicab drivers. Criminal history information might be relevant when hiring a worker in a child care facility or a kindergarten teacher.
Transparency, however, can come into tension with privacy. Can both of these important values be reconciled? Before turning to this question, I must first address how the privacy problem to which public records contribute should be understood. We must rethink certain longstanding notions about privacy before we can reach an appropriate balance between transparency and privacy.

**Conceptualizing Privacy and Public Records**

*Access: The Public Is Private.* The secrecy paradigm, as discussed in chapter 3, is deeply entrenched in information privacy law. In addition to focusing on whether information is completely secret or not, the paradigm categorizes information as either public or private. When information is private, it is hidden, and as long as it is kept secret, it remains private. When it is public, it is in the public domain available for any use. Information is seen in this black-and-white manner; either it is wholly private or wholly public.

This paradigm is outmoded in the Information Age. Unless we live as hermits, there is no way to exist in modern society without leaving information traces wherever we go. Therefore, we must abandon the secrecy paradigm. Privacy involves an expectation of a certain degree of accessibility of information. Under this alternative view, privacy entails control over and limitations on certain uses of information, even if the information is not concealed. Privacy can be violated by altering levels of accessibility, by taking obscure facts and making them widely accessible. Our expectation of limits on the degree of accessibility emerges from the fact that information in public records has remained relatively inaccessible until recently. Our personal information in public records remained private because it was a needle in a haystack, and usually nobody would take the time to try to find it. This privacy is rapidly disappearing as access to information is increasing.

In limited contexts, some courts are beginning to abandon the secrecy paradigm, although most courts still cling to it. In *United States Department of Justice v. Reporters Committee for Freedom of the Press*, the Supreme Court held that the release of FBI “rap sheets” was an invasion of privacy within the privacy exemption of FOIA. The FBI rap
sheets contained the date of birth, physical description, and a history of arrests, charges, and convictions on over 24 million people. The reporters argued that the rap sheet wasn’t private because it was merely a collection of data that had previously been publicly disclosed. The Court didn’t agree, noting that “there is a vast difference between the public records that might be found after a diligent search of courthouse files, county archives, and local police stations throughout the country and a computerized summary located in a single clearing-house of information.”

In cases involving the privacy torts, a few courts have recognized a privacy interest in information exposed to the public. In Melvin v. Reid, a former prostitute who was once criminally prosecuted for murder had left the prostitution business long ago and got married. When the movie The Red Kimono, depicted her life story and used her maiden name, she sued under the tort of public disclosure. The court held that although she could not claim that the facts about her life were private because they were in the public record, there was no need for the movie to use her real name.

Likewise, in Briscoe v. Reader’s Digest Ass’n, an article in Reader’s Digest magazine about hijacking disclosed that the plaintiff had hijacked a truck 11 years earlier. Briscoe had rehabilitated himself, and his new friends, family, and young daughter weren’t aware of his crime. The court held that although the facts of the crime could be disclosed, Briscoe could sue for the use of his name, which had no relevance to the article.

Generally, however, most courts still adhere to the secrecy paradigm and do not recognize a privacy interest when information is exposed to the public. As a result, most courts have rejected the Reid and Briscoe approach. In Forsher v. Bugliosi, the court considered Briscoe “an exception to the more general rule that ‘once a man has become a public figure, or news, he remains a matter of legitimate recall to the public mind to the end of his days.’” Likewise, the Restatement for the tort of public disclosure explains: “There is no liability when the defendant merely gives further publicity to information about the plaintiff that is already public. Thus there is no liability for giving publicity to facts about the plaintiff’s life which are matters of public record.” Similarly, for the tort of intrusion upon
seclusion, the Restatement provides that “there is no liability for the examination of a public record concerning the plaintiff.” Further, *Briscoe* seems foreclosed by the Supreme Court’s decision in *Cox Broadcasting Corp. v. Cohn*, which held that when information is disclosed in documents open to the public, the press cannot be punished for publishing it.

In a number of cases, courts applying the constitutional right to information privacy have become mired in the secrecy paradigm. Courts have refused to find a constitutional right to information privacy for data exposed to the public. In *Scheetz v. Morning Call, Inc.*, a court held that a husband and wife had no constitutional right to information privacy in a police report disclosed to the press containing the wife’s allegations of spousal abuse. Although her complaint to the police did not result in charges, “[t]he police could have brought charges without her concurrence, at which point all the information would have wound up on the public record, where it would have been non-confidential.” In *Cline v. Rogers*, the court held that police records weren’t private “since arrest and conviction information are matters of public record.” In *Walls v. City of Petersburg*, public employees were questioned about the criminal histories of their family members, their complete marital history, including marriages, divorces, and children, and any outstanding debts or judgments against them. According to the court, the information wasn’t private because it was already available in public records.

Courts have also adhered to the secrecy paradigm in challenges to Megan’s Laws, which mandate the public disclosure of information about prior sex offenders. In *Russell v. Gregoire*, convicted sex offenders challenged the disclosure of their picture, name, age, date of birth, crimes, and neighborhoods in which they lived. The court held that the information wasn’t private because it was “already fully available to the public.” Likewise, in *Paul P. v. Verniero*, the court held there was no privacy interest in the names and physical descriptions of previously convicted sex offenders.

In sum, although divided, most courts adhere to the secrecy paradigm. Unless the secrecy paradigm is abandoned, people will lose any ability to claim a privacy interest in the extensive personal information in public records.
Aggregation: The Digital Biography. Another longstanding notion of privacy—the invasion conception, which I discussed in chapter 6—doesn’t recognize an infringement of privacy unless there is a palpable invasion. Information protected as private must be embarrassing or harmful to one’s reputation. The problem with the invasion conception is that public record information often consists of fairly innocuous details—such as one’s birth date, address, height, weight, and so on.

Following the invasion conception, a number of courts have rejected claims that certain information falls within state FOIA privacy exemptions because the information didn’t pose immediate harms to reputation or security. One court reasoned that “[n]ames and addresses are not ordinarily personal, intimate, or embarrassing pieces of information.” Another court held that police payroll records containing each employee’s name, gender, date of birth, salary, and other data could be disclosed because the records didn’t harm their reputations. Information about teacher salaries, according to one court, didn’t fall within the privacy exemption because “[t]he salaries of public employees and schoolteachers are not ‘intimate details . . . the disclosure of which might harm the individual.’”

If the release of certain information in public records doesn’t make one blush or reveal one’s deepest secrets, then what is the harm? The harm stems from the aggregation effect discussed in chapter 3. Viewed in isolation, each piece of our day-to-day information is not all that telling; viewed in combination, it begins to paint a portrait about our personalities. Moreover, these digital biographies greatly increase our vulnerability to a variety of dangers. As public record information becomes more readily available, criminals can use it to gain access to a person’s financial accounts. For example, one industrious criminal gained access to the financial accounts of a number of individuals on Forbes magazine’s list of the 400 richest people in America such as Oprah Winfrey and George Lucas. Identity thieves frequently obtain personal information necessary for their criminal activity through information brokers, who sell reports about individuals based on public record data combined with other information. As discussed in chapter 6, the SSN is the most useful tool of the identity thief, and SSNs are often available in various public records.
Public record information also can expose people to violence. In 1989, a fan obsessed with actress Rebecca Shaeffer located her home address with the help of a private investigator who obtained it from California motor vehicles records. The fan murdered her outside her home. This killing spurred Congress to pass the Driver’s Privacy Protection Act (DPPA), which restricts the states’ ability to release motor vehicle records. In another example, an Internet site known as the “Nuremberg Files” posted information about doctors working in abortion clinics, including names, photos, SSNs, home addresses, descriptions of their cars, and information about their families. Doctors who were killed had a black line drawn through their names. Names of wounded doctors were shaded in gray. The doctors sued. At trial, they testified as to how their lives became riddled with fear, how some wore bulletproof vests and wigs in public. They won the suit and were able to block the use of their personal information on the website. This case demonstrates the dangers from increased access to personal information, even relatively non-intimate information such as one’s address.

At a more abstract level, the existence of digital dossiers alters the nature of the society we live in. In 1971, in his highly influential book, The Assault on Privacy, law professor Arthur Miller warned of the “possibility of constructing a sophisticated data center capable of generating a comprehensive womb-to-tomb dossier on every individual and transmitting it to a wide range of data users over a national network.” On a number of occasions, the federal government has flirted with the idea of creating a national database of personal information. The Johnson administration contemplated creating a National Data Center that would combine information collected by various federal agencies into one large computer database, but the plan was scrapped after a public outcry arose. Again, in the early 1970s, an official in the General Services Administration proposed that all of the federal government’s computer systems be connected in a network called FEDNET. Responding to a public outcry, Vice President Gerald Ford stopped the plan.

Although these proposals have been halted due to public outcries, we have been inching toward a system of de facto national identification for some time and are precariously close to having one.
Immigration Reform and Control Act of 1986 requires new employees to supply identification and proof of U.S. citizenship before obtaining a new job.\textsuperscript{34} In a recent effort to track down parents who fail to pay child support, the federal government has created a vast database consisting of information about all people who obtain a new job anywhere in the nation. The database contains their SSNs, addresses, and wages.\textsuperscript{35} The ready availability of one’s SSN and the ability to combine it with a host of other information about individuals will make increasingly more possible a reality where typing an individual’s name into a searchable database will pull up a “womb-to-tomb” dossier.

Such a reality can pose significant dangers. “Identity systems and documents,” observes political scientist Richard Sobel, “have a long history of uses and abuses for social control and discrimination.”\textsuperscript{36} Slaves were required to carry identifying papers to travel; identification cards were used by the Nazis in locating Jews; and the slaughter of Tutsis in Rwanda was aided by a system of identifiers.\textsuperscript{37} In addition to facilitating the monitoring and control of individuals, such a dossier may make a person a “prisoner of his recorded past.”\textsuperscript{38} Records of personal information can easily be used by government leaders and officials for improper monitoring of individuals. Data can be exploited for whatever task is at hand—a tool available to anyone in power in government to use in furtherance of the current passion or whim of the day. For example, in 1942, the Census Bureau used its data from the 1940 census to assist in the effort to intern Japanese Americans during World War II.\textsuperscript{39} Currently, we do not know the full consequences of living in a dossier society, but we are rapidly moving toward becoming such a society without sufficient foresight and preparation.

The problems and dangers just illustrated are not merely the product of the actions of the government. Rather, these troubles are caused by the way that both public- and private-sector entities are using personal information. The issue concerns more than isolated threats and harms, but is fundamentally about the structure of our society. Not only are public records altering the power that the government can exercise over people’s lives, but they are also contributing to the growing power of businesses. As I discussed earlier in this
book, although people may be aware that dossiers are being assembled about them, they have no idea what information the dossiers contain or how the dossiers are being used. This reality leads to unease, vulnerability, and powerlessness—a deepening sense that one is at the mercy of others, or, perhaps even more alarming, at the mercy of a bureaucratic process that is arbitrary, irresponsible, opaque, and indifferent to people’s dignity and welfare.

The problem with information collection and use today is not merely that individuals are no longer able to exercise control over their information; it is that their information is subjected to a bureaucratic process that is itself out of control. Without this process being subject to regulation and control and without individuals having rights to exercise some dominion over their information, individuals will be routinely subjected to the ills of bureaucracy.

Public records contribute to this privacy problem because they are often a principal source of information for businesses in the construction of their databases. Marketers stock their databases with public record information, and the uses to which these databases are put are manifold and potentially limitless. The personal information in public records is often supplied involuntarily and typically for a purpose linked to the reason why particular records are kept. The problem is that, often without the individual’s knowledge or consent, the information is then used for a host of different purposes by both the government and businesses.

Therefore, the privacy problem caused by public records concerns the structure of information flow—the way that information circulates throughout our society. The problem is not necessarily the disclosure of secrets or the injury of reputations, but is one created by increased access and aggregation of data. Privacy is an issue that concerns what type of society we want to construct for the future. Do we want to live in a Kafkaesque world where dossiers about individuals circulate in an elaborate underworld of public- and private-sector bureaucracies without the individual having notice, knowledge, or the ability to monitor or control the ways the information is used?
Transparency and Privacy: Reconciling the Tension

How can the tension between transparency and privacy be reconciled? Must access to public records be sacrificed at the altar of privacy? Or must privacy evaporate in order for government to be disinfected by sunlight?

Both transparency and privacy can be balanced through limitations on the access and use of personal information in public records. Of course, we must rethink what information belongs in public records. But we must also regulate the uses of our digital dossiers. The government is not doing enough to protect against the uses of the information that it routinely pumps into the public domain. If we abandon the notion that privacy is an exclusive status, and recognize that information in public records can still remain private even if there is limited access to it, then we can find a workable compromise for the tension between transparency and privacy. We can make information accessible for certain purposes only. When government discloses information, it can limit how it discloses that information by preventing it from being amassed by companies for commercial purposes, from being sold to others, or from being combined with other information and sold back to the government.

Much of the personal information in public records is not necessary to shed light on the way government carries out its functions. Rather, this information reveals more about the people who are the subjects of the government’s regulatory machinery. Although the federal FOIA has served to shed light on government activities and has supplied critical information for hundreds of books and articles, it has also been used as a tool for commercial interests. The vast majority of FOIA requests are made by businesses for commercial purposes.40 According to Judge Patricia Wald, FOIA turns agencies into “information brokers” rather than “a window for public assessment of how government works.”41 When weighing interests under the privacy exceptions to the federal FOIA, although courts can’t consider the identity and purpose of the requester, they can take into account the relationship of the requested document to the purposes of FOIA.42 Unlike the federal FOIA, many states routinely permit access by infor-
State FOIAs generally do not permit any discrimination among requesters. In a number of cases, officials wanting to restrict access to people requesting records for commercial use had no statutory authority to do so. In *Dunhill v. Director, District of Columbia Department of Transportation*, a marketer of personal information about individuals sought a listing on computer tape of the names, addresses, birth dates, gender, and expiration date of drivers’ permits of all people holding valid District of Columbia drivers’ permits. The court held that the government had to release the information because the statute didn’t authorize the government to look to the motives of the request.\(^43\) In *In re Crawford*, a preparer of bankruptcy petitions for debtors challenged the requirement that he divulge his SSN on the petition, which would then be made public. The court recognized that although disclosure of his SSN exposed him to potential fraud and identity theft, the interest in public access “is of special importance in the bankruptcy arena, as unrestricted access to judicial records fosters confidence among creditors regarding the fairness of the bankruptcy system.”\(^44\) Thus, the court formalistically invoked the principle of transparency, relying on the vague argument that total transparency fosters “confidence.”

The danger with any principle is that it can drift to different uses over time. Jack Balkin identifies this problem as “ideological drift.” “Ideological drift in law means that legal ideas and symbols will change their political valence as they are used over and over again in new contexts.”\(^45\) Laws fostering transparency are justified as shedding light into the dark labyrinths of government bureaucracy to expose its inner workings to public scrutiny, and preventing the harrowing situation in Kafka’s *The Trial*—a bureaucracy that worked in clandestine and mysterious ways, completely unaccountable and unchecked. These are certainly laudable goals, for they are essential to democracy and to the people’s ability to keep government under control. However, freedom of information laws are increasingly becoming a tool for powerful corporations to collect information about individuals to further their own commercial interests, not to shed light on the
government. A window to look in on the government is transforming into a window for the government and allied corporations to peer in on individuals. The data collected about individuals is then subject to a bureaucratic process that is often careless, uncontrolled, and clandestine. Because private-sector bureaucracies lack the transparency of government bureaucracies, there is a greater potential for personal information to be abused. Paradoxically, a right of access designed to empower individuals and protect them from the ills of bureaucracy can lead to exactly the opposite result.

There are certainly instances where information about individuals can illuminate government functioning. Examination of accident reports may reveal widespread problems with particular vehicles. Scrutiny of police records may indicate problems in police investigation and enforcement. Information about the salaries of public officials and employees allows the public to assess whether they are being over- or under-compensated. Disciplinary information about public employees allows taxpayers to scrutinize the performance of those who are earning their tax dollars. However, many of these purposes can be achieved through evaluating aggregate statistical data or by examining records with redacted personal identifying information.

The solution is not to eliminate all access to public records, but to redact personal information where possible and to regulate specific uses of information. Real property information must be made available for certain purposes, but it should not be available for all purposes. A person may need to obtain the address of a celebrity to serve process in a lawsuit; however, disclosing the address to fans or on the Internet is different.

Use restriction laws, such as those discussed in chapter 7, are a step in the right direction. These laws attempt to navigate the tension between transparency and privacy by permitting the use of public record information for certain purposes but not all purposes. One of the longstanding Fair Information Practices is purpose specification—that personal information obtained for one purpose cannot be used for another purpose without an individual’s consent. Often the purposes for the government collection of personal information vary widely from the purposes for which the data is used after it is disclosed in public records. Governments collecting personal informa-
tion should limit such uncontrolled drift in use. Access should be granted for uses furthering traditional functions of transparency such as the watchdog function; access should be denied for commercial solicitation uses because such uses do not adequately serve the functions of transparency. Rather, these uses make public records a cheap marketing tool, resulting in the further spread of personal information, which is often resold among marketers.

Use restriction laws must go beyond basic restrictions on access for commercial solicitation. The use of public records by information brokers or other entities that aggregate personal information and sell it to others is deeply problematic for the reasons discussed earlier in this chapter. Although information brokers have brought a new level of accessibility to public records, they have also contributed greatly to the creation of digital dossiers. This type of aggregated public record information is often not used for the purposes of checking governmental abuse or monitoring governmental activities. Rather, it is used to investigate individuals. This investigation is at the behest of other individuals, private detectives, employers, and law enforcement officials. Information brokers such as ChoicePoint collect public record information and supplement it with a host of other personal information, creating a convenient investigation tool for government entities. The use of information brokers by the government to investigate citizens runs directly counter to the spirit of freedom of information laws, which were designed to empower individuals to monitor their government, not vice versa.

Certain information should be restricted from public records completely. The proposal by the Administrative Office of the U.S. Court System to separate both paper and electronic documents into a public and private file for civil cases and to restrict access to certain documents in criminal proceedings such as pre-sentence reports is a step in the right direction.\textsuperscript{47} One example of information that should be excluded from public records is a person’s SSN.\textsuperscript{48} SSNs serve as a gateway to highly sensitive information such as financial accounts, school records, and a host of other data. As a routine practice, SSNs should be redacted from every document before being disclosed publicly.

Jurors, parties to litigation, and witnesses should all be informed of the extent to which their personal information could become a public
record and must be given an opportunity to voice their privacy concerns and have information redacted.

Of course, provisions in the law can be made for people who want to consent to the disclosure of their personal information. If the requester desires personal information about a specific individual in a specific case, the agency or court can contact the individual, inform her of the purpose of the request, and ask if she consents to disclosure. People may want to consent if the data is being used by a researcher, but may not if the information is requested for marketing purposes.

The federal Privacy Act must be amended to provide more meaningful protection. Its restrictions on the use of SSNs must be strengthened to regulate and restrict the use of SSNs by the private sector. Thus, the Privacy Act should prohibit the use of SSNs as identifiers by businesses, schools, and hospitals. Further, the Privacy Act should contain meaningful remedies for violations. People should be permitted to sue for negligent infringements of the Act—not just willful ones. Rarely do government agencies willfully disclose personal information in violation of the Privacy Act; most disclosures occur because of carelessness and inadvertence. By expanding the Act in this way, agencies will have a strong incentive to treat their record systems with more care and to provide greater security for the personal information they maintain. Government agency information-handling practices should be routinely audited by a governmental oversight agency. Moreover, the “routine use” exception must be significantly tightened.

Finally, more laws like the Driver’s Privacy Protection Act are necessary to ensure that states maintain adequate privacy protection in their public records law. A federal baseline should not preempt states from adopting stricter protections of privacy, but it must provide a meaningful floor of protection. Although each state should adopt its own statute akin to the federal Privacy Act, one option would be to extend the federal Privacy Act to the states.

We may never be able to achieve complete secrecy of information in many situations and, in some situations, complete secrecy would be undesirable. But we can limit accessibility and use.
Public Records and the First Amendment

Do the access and use restrictions I propose pass muster under the First Amendment? Understood broadly, the First Amendment protects openness in information flow. First, the Court has held that the First Amendment provides certain rights of access to at least some government proceedings. Restrictions on the information available in public records might infringe upon this right. Second, freedom of speech prevents the government from restricting the disclosure and dissemination of information. A close analysis of the Court’s decisions, however, reveals that access and use restrictions are constitutional.

The Right of Access. The Supreme Court has held that the First Amendment mandates that certain government proceedings be open to the public. In Richmond Newspapers, Inc. v. Virginia, a plurality of the Court concluded that the public had a First Amendment right of access to criminal trials.49 Two years later, in Globe Newspaper Co. v. Superior Court, the Court struck down a law closing criminal trials when juvenile sexual assault victims testified. According to the Court, a “major purpose” of the First Amendment is “to protect the free discussion of governmental affairs.” The Court articulated a two-pronged test to determine whether the right to access applies, first looking to whether the proceeding “historically has been open to the press and general public” and then examining whether access “plays a particularly significant role in the functioning of the judicial process and the government as a whole.”50 Shortly after Globe, the Court extended the right to access beyond the immediate criminal trial to jury selection and to pretrial proceedings.51 Lower courts have proclaimed that the right of access applies to hearings for pretrial suppression, due process, entrapment, and bail.52

Although the Court has never squarely addressed whether the right of access applies beyond the criminal arena, several lower courts have extended it to civil cases. For example, in Publicker Industries, Inc. v. Cohen, the court reasoned that “the civil trial, like the criminal trial, plays a particularly significant role in the functioning of the judicial
process and the government as a whole. Several courts have even concluded that the right to access “extends to at least some categories of court documents and records,” but not all courts agree. Although courts have rarely applied the right of access beyond court records, since the rationale for the right is to provide knowledge about the workings of the government, the right might logically extend to other public records. Even under such an expansive view, however, the right of access shouldn’t prohibit many access and use restrictions. When public records illuminate government functioning, access to them is generally consistent with the rationale for the right of access. However, the grand purposes behind the right are not present in the context of much information gathering from public records today. Public records are becoming a tool for powerful companies to use in furtherance of commercial gain. These uses do not shed light on the government.

In fact, the Constitution does not simply require open information flow; it also establishes certain responsibilities for the way that the government uses the information it collects. The Court has held that there are circumstances where the government cannot force individuals to disclose personal information absent a compelling government interest. In *NAACP v. Alabama*, the Court struck down a statute requiring the NAACP to disclose a list of its members because this could expose them to potential economic reprisal and physical violence, thus chilling their freedom of association. Similarly, in *Greidinger v. Davis*, the Fourth Circuit held that Virginia’s voter registration system was unconstitutional because it forced people to publicly disclose their SSNs in order to vote, thus deterring people from voting by exposing them to potential harms such as identity theft and fraud. These cases establish that government disclosure of personal information it has collected can be unconstitutional when it interferes with the exercise of fundamental rights.

Further, under the constitutional right to privacy, the Court has held that government has a duty to protect privacy when it collects personal data. In *Whalen v. Roe*, which I discussed in chapter 4, the Court held that the right to privacy encompassed the protection of personal information:
We are not unaware of the threat to privacy implicit in the accu-
mulation of vast amounts of personal information in computer-
ized data banks or other massive government files. . . . The right
to collect and use such data for public purposes is typically ac-
companied by a concomitant statutory or regulatory duty to
avoid unwarranted disclosures. . . . [I]n some circumstances that
duty arguably has its roots in the Constitution.57

*Whalen* recognized that when the government collects personal in-
formation, it has a responsibility to keep it secure and confidential.

Since its creation in *Whalen*, the constitutional right to informa-
tion privacy has begun to evolve in the courts, but it is still in the early
stages of growth.58 The full extent of the government’s responsibilities
in handling personal data awaits further development. Based on the
cases decided thus far, the Constitution requires public access when
information will shed light on the functioning of the government, and
it requires confidentiality when information pertains to the personal
lives of individuals.

**Freedom of Speech.** The First Amendment more directly fosters infor-
mation flow about government activities by forbidding restrictions on
freedom of speech. Understanding how use and access restrictions
on public record information interact with the First Amendment re-
quires a difficult navigation through a number of cases. In one series
of cases, the Court has struck down statutes prohibiting the disclo-
sure of information gleaned from public records. In *Cox Broadcasting
Corp. v. Cohn*, the Court held that a state could not impose civil liabil-
ity based upon publication of a rape victim’s name obtained from a
court record: “Once true information is disclosed in public court doc-
uments open to public inspection, the press cannot be sanctioned for
publishing it.” Punishing the press for publishing public record infor-
mation would “invite timidity and self-censorship and very likely lead
to the suppression of many items that would otherwise be published
and that should be made available to the public.”59 In *Smith v. Daily
Mail*, the Court struck down a statute prohibiting the publication of
the names of juvenile offenders: “[I]f a newspaper lawfully obtains
truthful information about a matter of public significance then state officials may not constitutionally punish publication of the information, absent a need to further a state interest of the highest order.”

This line of cases culminated in *Florida Star v. B.J.F.* in which a newspaper published the name of a rape victim, which it obtained from a publicly released police report. The report was in a room with signs stating that rape victims’ names weren’t part of the public record and weren’t to be published. The reporter even admitted that she knew she wasn’t allowed to report on the information. When the story ran, many of the victim’s friends learned about her rape, and a man made threatening calls to her home. As a result, she had to change her phone number and residence, seek police protection, and obtain mental health counseling. Based upon a Florida law prohibiting the disclosure of rape victims’ names, a jury found the paper liable. The Supreme Court, however, held that the verdict ran afoul of the newspaper’s First Amendment rights.61 Taken together, these cases support the premise that once the government makes information public, the government cannot subsequently sanction its further disclosure.

However, in *Los Angeles Police Department v. United Reporting Publishing Co.*, the Court upheld a law restricting access for public arrestee information. Requesters of the information had to declare under penalty of perjury that the address information would not be used “directly or indirectly to sell a product or service.” Rejecting a challenge that the law infringed upon commercial speech, the Court reasoned that the statute was not “prohibiting a speaker from conveying information that the speaker already possesses” but was merely “a governmental denial of access to information in its possession.” As long as the government doesn’t have a duty to provide access to information, it can selectively determine who can obtain it.62

The Court’s jurisprudence thus creates a distinction between pre-access conditions on obtaining information and post-access restrictions on the use or disclosure of the information. If the government is not obligated to provide access to certain information by the First Amendment, it can amend its public access laws to establish pre-access conditions, restricting access for certain kinds of uses. Governments can make a public record available on the condition that
certain information is not disclosed or used in a certain manner. However, once the information is made available, governments cannot establish post-access restrictions on its disclosure or use.

The Court’s distinction between pre-access and post-access restrictions seems rather tenuous. States can easily redraft their statutes to get around *Florida Star*. For example, Florida could rewrite its law to make rape victims’ names available on the condition that the press promise the names not be disclosed. Conditional access and use restrictions thus appear to be an end-run around *Florida Star*. Can the Court’s distinction between pre- and post-access restrictions be defended?

I believe it can. First, in *Florida Star*, the Court was concerned about the government’s failure “to police itself in disseminating information.” The mistake was made by the police department in failing to redact the name, and thus it was unfair “to sanction persons other than the source of its release.” In contrast, with pre-access restrictions, the government is taking the appropriate care to protect the information itself.

Second, in both *Cox* and *Florida Star*, the Court was concerned about the chilling effects to speech from the uncertainty over whether certain public record information could be disclosed. Pre-access restrictions alleviate these concerns. Since the recipient of the information has to expressly agree to any restrictions on using the information beforehand, she will be on clear notice as to her obligations and responsibilities in handling the data.

Third, and most importantly, the distinction is a good practical compromise. Without a distinction between post- and pre-access conditions, the government would be forced into an all-or-nothing tradeoff between transparency and privacy. The government could make records public, allowing all uses of the personal information, or the government could simply not make records available at all. By making access conditional on accepting certain responsibilities when using data, the public can have access to a wide range of records while privacy remains protected at the same time.

Has the Court too quickly dispatched with the free speech implications of conditional or limited access regulation? For example, some argue that restrictions on commercial access are unconstitutional
content-based restrictions on free speech because they single out specific messages and viewpoints—namely, commercial ones. Dissenting in United Reporting Publishing Corp., Justice Stevens argued that the California access and use restriction improperly singled out “a narrow category of persons solely because they intend to use the information for a [commercial] purpose.”64 However, commercial access restrictions are not being applied because of disagreement with the message that commercial users wish to send. Nor do they favor a particular speaker or specific ideas. Although particular categories of use (i.e., commercial) are being singled out, avoiding viewpoint discrimination does not entail avoiding all attempts to categorize or limit uses of information. Indeed, the First Amendment constitutional regime depends upon categorizing speech. The Supreme Court protects certain categories of speech much less stringently than other forms of speech. Obscene speech, words that incite violence, and defamatory speech about private figures all receive minimal protection.65 Commercial speech is also singled out, safeguarded with only an intermediate level of scrutiny.66 Although there is no bright line that distinguishes when certain categories map onto particular viewpoints to such a degree as to constitute discrimination based on viewpoint, the category of commercial speech is broad enough to encompass a multitude of viewpoints and is a category that forms part of the architecture of the current constitutional regime.

Therefore, governments should be able to restrict access for certain purposes or condition access on an enforceable promise not to engage in certain uses of information. Of course, it would be improper for the government to single out particular viewpoints. Thus, for example, governments should not restrict access to public records to those who wish to use the information to advocate for certain causes rather than others. Nor could the government restrict access based on the particular beliefs or ideas of the person or entities seeking access to the information. In short, the government can't single out certain uses because it dislikes the ideas or views of a particular speaker. A limitation on commercial use is broad enough to encompass a diverse enough range of viewpoints, and the government is merely limiting uses of information rather than the expression of particular ideas.
Public Records in the Information Age. Public records are increasingly posing a serious threat to privacy in the Information Age. To understand this threat, our conceptions of privacy must be adapted to today’s technological realities. We must abandon the secrecy paradigm and recognize that what is public can be private—not in the sense that it is secret, but in the limitation of the uses and disclosures of the information. Privacy is about degrees of accessibility. The threat to privacy is not in isolated pieces of information, but in increased access and aggregation, the construction of digital dossiers and the uses to which they are put. States must begin to rethink their public record regimes, and the federal government should step in to serve as the most efficient mechanism to achieve this goal. It is time for the public records laws of this country to mature to meet the problems of the Information Age.