the digital person

TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE

daniel j. solove

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

NEW YORK UNIVERSITY PRESS *New York and London*

new york university press
New York and London
www.nyupress.org

Library of Congress Cataloging-in-Publication Data
Solove, Daniel J., 1972–
The digital person :
technology and privacy in the information age / Daniel J. Solove.
p. cm.—(Ex machina)
Includes bibliographical references and index.
ISBN 0–8147–9846–2 (cloth : alk. paper)
1. Data protection—Law and legislation—United States.
2. Electronic records—Access control—United States.
3. Public records—Law and legislation—United States.
4. Government information—United States.
5. Privacy, Right of—United States. I. Title. II. Series.
KF1263.C65S668 2004
343.7308'58—dc22 2004010188

New York University Press books are printed on acid-free paper,
and their binding materials are chosen for strength and durability.

Manufactured in the United States of America

10 9 8 7 6 5 4 3 2 1

In loving memory of

my grandma,

Jean

Contents

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.

9 Government Information Gathering

Thus far, I have discussed how personal information is being more readily collected, stored, transferred, and combined with other information. Part I of this book discussed the problems of information flow among various businesses, and part II focused on information flows from the government to the private sector. But there is another problematic type of information flow that is rapidly escalating—data transfers from the private sector to the government. The vast digital dossiers being constructed by businesses are becoming an increasingly desirable resource for law enforcement officials. And this threatens to transform the relationship between government and citizen in some very troubling ways.

Third Party Records and the Government

Earlier in this book, I described the extensive amount of information that companies are stockpiling about us. To live in the modern world, we must enter into numerous relationships with other people and businesses: doctors, lawyers, businesses, merchants, magazines,

newspapers, banks, credit card companies, employers, landlords, ISPs, insurance companies, phone companies, and cable companies. The list goes on and on. Our relationships with all of these entities generate records containing personal information necessary to establish an account and record our transactions and preferences. We are becoming a society of records, and these records are not held by us, but by third parties.

These record systems are becoming increasingly useful to law enforcement officials. Personal information can help the government detect fraud, espionage, fugitives, drug distribution rings, and terrorist cells. Information about a person's financial transactions, purchases, and religious and political beliefs can assist the investigation of suspected criminals and can be used to profile people for more thorough searches at airports.

The government, therefore, has a strong desire to obtain personal information found in records maintained by third parties. For instance, from pen registers and trap and trace devices, the government can obtain a list of all the phone numbers dialed to or from a particular location, potentially revealing the people with whom a person associates. From bank records, which contain one's account activity and check writing, the government can discover the various companies and professionals that a person does business with (ISP, telephone company, credit card company, magazine companies, doctors, attorneys, and so on). Credit card company records can reveal where one eats and shops. The government can obtain one's travel destinations and activities from travel agent records. From hotel records, it can discover the numbers a person dialed and the pay-per-view movies a person watched.[1] The government can obtain one's thumbprint from car rental companies that collect them to investigate fraud.[2] From video stores, the government can access an inventory of the videos that a person has rented.

The government can also glean a wealth of information from the extensive records employers maintain about their employees.[3] Employers frequently monitor their employees.[4] Some use software to track how employees surf the Internet.[5] Employers often record information about an employee's email use, including back-up copies of the contents of email. A number of employers also conduct drug test-

ing, and many require prospective employees to answer questionnaires asking about drug use, finances, psychological treatment, marital history, and sexuality.[6] Some even require prospective hires to take a psychological screening test.[7]

Landlords are another fertile source of personal information. Landlord records often contain financial, employment, and pet information, in addition to any tenant complaints. Many landlords also maintain log books at the front desk where visitors sign in. Some apartment buildings use biometric identification devices, such as hand scanners, to control access to common areas such as gyms.

Increasingly, companies and entities that we have never established any contact with nevertheless have dossiers about us. Credit reporting agencies maintain information relating to financial transactions, debts, creditors, and checking accounts. The government can also find out details about people's race, income, opinions, political beliefs, health, lifestyle, and purchasing habits from the database companies that keep extensive personal information on millions of Americans.

Beyond the records described here, the Internet has the potential to become one of the government's greatest information gathering tools. There are two significant aspects of the Internet that make it such a revolutionary data collection device. First, it gives many individuals a false sense of privacy. The secrecy and anonymity of the Internet is often a mirage. Rarely are people truly anonymous because ISPs keep records of a subscriber's screen name and pseudonyms. ISP account information includes the subscriber's name, address, phone numbers, passwords, information about web surfing sessions and durations, and financial information.[8] By learning a person's screen name, the government can identify who posted messages in newsgroups or conversed in chatrooms.

At the government's request, an ISP can keep logs of the email addresses with which a person corresponds. Further, if a person stores email that is sent and received with the ISP, the government can obtain the contents of those emails.

Second, the Internet is unprecedented in the degree of information that can be gathered and stored. It is one of the most powerful generators of records in human history. As discussed in chapter 2, websites

often accumulate a great deal of information about their users, from transactional data to information collected through cookies. The government can glean a substantial amount of information about visitors to a particular website. From Internet retailers, the government can learn about the books, videos, music, and electronics that one purchases. Some Internet retailers, such as Amazon.com, record all the purchases a person has made throughout many years. Based on this information, the government can discover a consumer's interests, political views, religious beliefs, and lifestyle.

The government may also obtain information from websites that operate personalized home pages. Home pages enable users to keep track of the stocks they own, favorite television channels, airfares for favorite destinations, and news of interest. Other websites, such as Microsoft Network's calendar service, allow users to maintain their daily schedule and appointments. Further, as discussed in chapter 2, there are database companies that amass extensive profiles of people's websurfing habits.

While life in the Information Age has brought us a dizzying amount of information, it has also placed a profound amount of information about our lives in the hands of numerous entities. As discussed earlier, these digital dossiers are increasingly becoming digital biographies, a horde of aggregated bits of information combined to reveal a portrait of who we are based upon what we buy, the organizations we belong to, how we navigate the Internet, and which shows and videos we watch. This information is not held by trusted friends or family members, but by large bureaucracies that we do not know very well or sometimes do not even know at all.

Government–Private-Sector Information Flows

In late 2002, the news media reported that the Department of Defense was planning a project known as Total Information Awareness (TIA). The project was to be run by John Poindexter, who had been convicted in 1990 for his activities during the Iran-contra scandal. TIA envisioned the creation of a gigantic government database of personal information, including data culled from private-sector entities concerning finances, education, travel, health, and so on. This infor-

mation would then be analyzed under various models to detect patterns and profiles for terrorist activities.[9] The website for the project contained the symbol of a pyramid with beams of light emanating from an eye at the top. Next to the pyramid was a globe, illuminated by the light. Underneath the image were the words *scientia est potentia*—"knowledge is power."[10]

When TIA broke as a major news story, civil liberties groups and many commentators and politicians voiced stinging criticism. In a *New York Times* editorial, William Safire wrote that Poindexter "is determined to break down the wall between commercial snooping and secret government intrusion. . . . And he has been given a $200 million budget to create computer dossiers on 300 million Americans."[11] After these outcries, the pyramid and eye logo was quickly removed from the Department of Defense website. The Senate amended its spending bill in January 2003 to temporarily suspend funding for TIA until the details of the program were explained to Congress.[12] In May 2003, the Department of Defense issued its report to Congress, renaming the program "Terrorism Information Awareness" and declaring (without specifying how) that it would protect privacy. Later on, in July, the Senate voted unanimously to stop funding for TIA. The program had been killed.

But TIA is only one part of the story of government access to personal information and its creation of dossiers on American citizens. In fact, for quite some time, the government has been increasingly contracting with businesses to acquire databases of personal information. Database firms are willing to supply the information and the government is willing to pay for it. Currently, government agencies such as the FBI and IRS are purchasing databases of personal information from private-sector companies.[13] A private company called ChoicePoint, Inc. has amassed a database of 10 billion records and has contracts with at least 35 federal agencies to share the data with them. In 2000, the Justice Department signed an $8 million contract with ChoicePoint, and the IRS reached a deal with the company for between $8 and $12 million. ChoicePoint collects information from public records from around the country and then combines it with information from private detectives, the media, and credit reporting firms. This data is indexed by people's SSNs. The Center for Medicare

and Medicaid Services uses ChoicePoint's data to help it identify fraudulent Medicare claims by checking health care provider addresses against ChoicePoint's list of "high-risk and fraudulent business addresses." ChoicePoint's information is not only used by government agencies but also by private-sector employers to screen new hires or investigate existing employees.[14]

ChoicePoint's information is a mixture of fact and fiction. There are a number of errors in the records, such as when a ChoicePoint report falsely indicated that a woman was a convicted drug dealer and shoplifter, resulting in her being fired from her job.[15] ChoicePoint also had a hand in the 2000 presidential election problems in Florida. ChoicePoint supplied Florida officials with a list of 8,000 "ex-felons" to eliminate from their voter lists.[16] However, many of the 8,000 were not guilty of felonies, only misdemeanors, and were legally eligible to vote. Although the error was discovered prior to the election and officials tried to place the individuals back on the voter rolls, the error may have led to some eligible voters being turned away at the polls.

Additionally, many states have joined together to create a database system called Multi-State Anti-Terrorism Information Exchange, or MATRIX for short. Run by SeisInt, Inc., a private-sector company in Florida, MATRIX contains personal information gathered from public records and from businesses. In its vast fields of data, MATRIX includes people's criminal histories, photographs, property ownership, SSNs, addresses, bankruptcies, family members, and credit information. The federal government has provided $12 million to help support the program.[17]

A second form of information flow from the private sector to the government emerges when the government requests private-sector records for particular investigations or compels their disclosure by subpoena or court order. Voluntary disclosure of customer information is within the third party company's discretion. Further, whether a person is notified of the request and given the opportunity to challenge it in court is also within the company's discretion.

The September 11, 2001 terrorist attacks changed the climate for private sector-to-government information flows. Law enforcement officials have a greater desire to obtain information that could be helpful in identifying terrorists or their supporters, including infor-

mation about what people read, the people with whom they associate, their religion, and their lifestyle. Following the September 11 attack, the FBI simply requested records from businesses without a subpoena, warrant, or court order.[18] Recently, Attorney General John Ashcroft has revised longstanding guidelines for FBI surveillance practices. Under the previous version, the FBI could monitor public events and mine the Internet for information only when "facts or circumstances reasonably indicate that a federal crime has been, is being, or will be committed."[19] Under the revised version, the FBI can engage in these types of information gathering without any requirement that it be part of a legitimate investigation or related in any manner to criminal wrongdoing. The FBI can now collect "publicly available information, whether obtained directly or through services or resources (whether nonprofit or commercial) that compile or analyze such information; and information voluntarily provided by private entities."[20] Further, the FBI can "carry out general topical research, including conducting online searches and accessing online sites and forums."[21]

In conjunction with the government's greater desire for personal information, the private sector has become more willing to supply it. Background check companies, for instance, experienced a large boost in business after September 11.[22] Several large financial companies developed agreements to provide information to federal law enforcement agencies.[23] Indeed, in times of crisis or when serious crimes are at issue, the incentives to disclose information to the government are quite significant. Shortly after September 11, around 200 universities admitted to giving the FBI access to their records on foreign students—often without a subpoena or court order.[24] In violation of its privacy policy, JetBlue Airlines shared the personal data of 1 million customers with Torch Concepts, an Alabama company contracting with the Defense Department to profile passengers for security risks. Torch combined the JetBlue data with SSNs, employment information, and other details obtained from Acxiom, Inc., a database marketing company.[25] In a similar incident, Northwest Airlines secretly turned over to NASA its customer data—including addresses, phone numbers, and credit card information—for use in a government data mining project.[26] In a December 2002 survey of nearly 800

chief security officers, almost 25 percent said that they would supply information to the government without a court order, with 41 percent doing so in cases involving national security.[27]

When businesses refuse to cooperate, the government can compel production of the information by issuing a subpoena or obtaining a court order. These devices are very different from warrants because they offer little protection to the individual being investigated. Notification of the target of the investigation is often within the discretion of the third party. Further, it is up to the third party to challenge the subpoena. So, rather than spend the money and resources to challenge the subpoena, companies can simply turn it over or permit the government to search their records. Since September 11, AOL and Earthlink, two of the largest ISPs, have readily cooperated with the investigation of the terrorist attacks.[28] Often, ISPs have their own technology to turn over communications and information about targets of investigations. If they lack the technology, law enforcement officials can install devices such as "Carnivore" to locate the information.[29] Carnivore, now renamed to the more innocuous "DCS1000," is a computer program installed by the FBI at an ISP.[30] It can monitor all ISP email traffic and search for certain keywords in the content or headers of the email messages.

These developments are troubling because private-sector companies often have weak policies governing when information may be disclosed to the government. The privacy policy for the MSN network, an affiliation of several Microsoft, Inc. websites such as Hotmail (an email service), Health, Money, Newsletters, eShop, and Calendar, states:

> MSN Web sites will disclose your personal information, without notice, only if required to do so by law or in the good faith belief that such action is necessary to: (a) conform to the edicts of the law or comply with legal process served on Microsoft or the site.[31]

Though somewhat unclear, this privacy policy appears to require a subpoena or court order for the government to obtain personal data.

Amazon.com's privacy policy reads: "We release account and other personal information when we believe release is appropriate to comply with law . . . or protect the rights, property, or safety of

Amazon.com, our users, or others."[32] It is unclear from this policy the extent to which Amazon.com, in its discretion, can provide information to law enforcement officials.

EBay, a popular online auction website, has a policy stating that

> [it] cooperates with law enforcement inquiries, as well as other third parties to enforce laws, such as: intellectual property rights, fraud and other rights. We can (and you authorize us to) disclose any information about you to law enforcement or other government officials as we, in our sole discretion, believe necessary or appropriate, in connection with an investigation of fraud, intellectual property infringements, or other activity that is illegal or may expose us or you to legal liability.[33]

This policy gives eBay almost complete discretion to provide the government with whatever information it deems appropriate.

Truste.com, a nonprofit organization providing a "trustmark" for participating websites that agree to abide by certain privacy principles, has drafted a model privacy statement that reads: "We will not sell, share, or rent [personal] information to others in ways different from what is disclosed in this statement."[34] The statement then says that information may be shared with "an outside shipping company to ship orders, and a credit card processing company to bill users for goods and services." Personal data is also shared with third parties when the user signs up for services that are provided by those third parties. This policy, however, does not contain any provision about supplying information to the government. Further, the policy does not inform people that under existing law, information must be disclosed to the government pursuant to a subpoena or court order.

The government is also increasing information flow from the private sector by encouraging it to develop new information gathering technologies. Private-sector firms stand to profit from developing such technologies. Since September 11, companies have expressed an eagerness to develop national identification systems and face-recognition technology.[35] In addition, the federal government has announced a "wish list" for new surveillance and investigation technologies.[36] Companies that invent such technologies can obtain lucrative government contracts.

The government has also funded private-sector information gathering initiatives. For instance, a company that began assembling a national database of photographs and personal information as a tool to guard against consumer fraud has received $1.5 million from the Secret Service to aid in the development of the database.[37]

In certain circumstances, where institutions do not willingly cooperate with the government, the law requires their participation. For example, the Bank Secrecy Act of 1970 forces banks to maintain records of financial transactions to facilitate law enforcement needs—in particular, investigations and prosecutions of criminal, tax, or regulatory matters.[38] All federally insured banks must keep records of each customer's financial transactions and must report to the government every financial transaction in excess of $10,000.[39] The Personal Responsibility and Work Opportunity Reconciliation Act of 1996 requires employers to report personal information from all new employees including SSNs, addresses, and wages.[40] The Communications Assistance for Law Enforcement Act of 1994 requires telecommunications service providers to develop technology to assist government surveillance of individuals.[41] Passed in 2001, the USA-PATRIOT Act authorizes the FBI to obtain a court order to inspect or seize "books, records, papers, documents, or other items" for use in an investigation for terrorism or intelligence activities.[42] This provision contains a gag order, prohibiting anybody from disclosing that the FBI has sought or obtained anything.[43]

All of this suggests that businesses and government have become allies. When their interests diverge, the law forces cooperation. The government can increasingly amass gigantic dossiers on millions of individuals, conduct sweeping investigations, and search for vast quantities of information from a wide range of sources, without any probable cause or particularized suspicion. Information is easier to obtain, and it is becoming more centralized. The government is increasingly gaining access to the information in our digital dossiers. As Justice Douglas noted in his dissent when the Court upheld the constitutionality of the Bank Secrecy Act:

> These [bank records] are all tied to one's SSN; and now that we have the data banks, these other items will enrich that store-

> house and make it possible for a bureaucrat—by pushing one button—to get in an instant the names of the 190 million Americans who are subversives or potential and likely candidates.[44]

Thus, we are increasingly seeing collusion, partly voluntary, partly coerced, between the private sector and the government. While public attention has focused on the Total Information Awareness project, the very same goals and techniques of the program continue to be carried out less systematically by various government agencies and law enforcement officials. We are already closer to Total Information Awareness than we might think.

The Orwellian Dangers

Although there are certainly many legitimate needs for law enforcement officials to obtain personal data, there are also many dangers to unfettered government access to information. There are at least two general types of harms, some best captured by the Orwell metaphor and others that are more fittingly described with the Kafka metaphor. I turn first to the Orwellian dangers.

Creeping toward Totalitarianism. Historically, totalitarian governments have developed elaborate systems for collecting data about people's private lives.[45] Although the possibility of the rise of a totalitarian state is remote, if our society takes on certain totalitarian features, it could significantly increase the extent to which the government can exercise social control. Justice Brandeis was prescient when he observed that people "are naturally alert to repel invasion of their liberty by evil-minded rulers. The greatest dangers to liberty lurk in the insidious encroachment by men of zeal, well-meaning but without understanding."[46]

Democracy and Self-Determination. Even if government entities are not attempting to engage in social control, their activities can have collateral effects that harm democracy and self-determination. Paul Schwartz illustrates this with his theory of "constitutive privacy." According to Schwartz, privacy is essential to both individuals and

communities: "[C]onstitutive privacy seeks to create boundaries about personal information to help the individual and define terms of life within the community." As a form of regulation of information flow, privacy shapes "the extent to which certain actions or expressions of identity are encouraged or discouraged." Schwartz contends that extensive government oversight over an individual's activities can "corrupt individual decision making about the elements of one's identity."[47] Likewise, Julie Cohen argues that a "realm of autonomous, unmonitored choice . . . promotes a vital diversity of speech and behavior." The lack of privacy "threatens not only to chill the expression of eccentric individuality, but also, gradually, to dampen the force of our aspirations to it."[48]

Freedom of Association. Government information collection interferes with an individual's freedom of association. The Court has held that there is a "vital relationship between freedom to associate and privacy in one's associations."[49] In a series of cases, the Court has restricted the government's ability to compel disclosure of membership in an organization.[50] In *Baird v. State Bar,*[51] for example, the Court has declared: "[W]hen a State attempts to make inquiries about a person's beliefs or associations, its power is limited by the First Amendment. Broad and sweeping state inquiries into these protected areas . . . discourage citizens from exercising rights protected by the Constitution."[52] The government's extensive ability to glean information about one's associations from third party records without any Fourth Amendment limitations threatens the interests articulated in these cases.[53]

Anonymity. Extensive government information gathering from third party records also implicates the right to speak anonymously. In *Talley v. California,* the Court struck down a law prohibiting the distribution of anonymous handbills as a violation of the First Amendment. The Court held that "[p]ersecuted groups and sects from time to time throughout history have been able to criticize oppressive practices and laws either anonymously or not at all." Further, the Court reasoned, "identification and fear of reprisal might deter perfectly peaceful discussions of public matters of importance."[54] The Court

has reiterated its view of the importance of protecting anonymous speech in subsequent cases.[55] From third parties, especially ISPs, the government can readily obtain an anonymous or pseudonymous speaker's identity. Only computer-savvy users can speak with more secure anonymity. Although private parties attempting to identify an anonymous speaker through subpoenas have been required to satisfy heightened standards,[56] no such heightened standards have yet been applied when the government seeks to obtain the information.

Further, beyond typical anonymity is the ability to receive information anonymously. As Julie Cohen persuasively contends: "The freedom to read anonymously is just as much a part of our tradition, and the choice of reading materials just as expressive of identity, as the decision to use or withhold one's name."[57] The lack of sufficient controls on the government's obtaining the extensive records about how individuals surf the web, the books and magazines they read, and the videos or television channels they listen to can implicate this interest.

Additionally, the increasing information flow between the private sector and the government not only impacts the privacy of the target of an investigation, but can also affect the privacy of other individuals. The names, addresses, phone numbers, and a variety of data about a number of individuals can be ensnared in records pertaining to the target.

These types of harms can inhibit individuals from associating with particular people and groups and from expressing their views, especially unpopular ones. This kind of inhibition is a central goal of Orwell's Big Brother. Although it certainly does not approach the same degree of oppressiveness as Big Brother, it reduces the robustness of dissent and weakens the vitality of our communication.

The Kafkaesque Dangers

The second general type of danger promoted by government information gathering consists of the harms routinely arising in bureaucratic settings: decisions without adequate accountability, dangerous pockets of unfettered discretion, and choices based on short-term goals without consideration of the long-term consequences or the larger social effects. These bureaucratic harms have similarities to

those I discussed earlier when discussing the Kafka metaphor, although these harms take on some new dimensions with government law enforcement bureaucracy. As in Kafka's *The Trial,* dossiers circulate throughout a large government bureaucracy, and individuals are not informed how their information is used and how decisions are made based on their data. The existence of dossiers of personal information in government bureaucracies can lead to dangers such as hasty judgment in times of crisis, the disparate impact of law enforcement on particular minorities, cover-ups, petty retaliation for criticism, blackmail, framing, sweeping and disruptive investigations, racial or religious profiling, and so on.

The most frequent problem is not that law enforcement agencies will be led by corrupt and abusive leaders, although this arguably happened for nearly 50 years when J. Edgar Hoover directed the FBI. The problem is the risk that judgment will not be exercised in a careful and thoughtful manner. In other words, it stems from certain forms of government information collection shifting power toward a bureaucratic machinery that is poorly regulated and susceptible to abuse. This shift has profound social effects because it alters the balance of power between the government and the people, exposing individuals to a series of harms, increasing their vulnerability and decreasing the degree of power they exercise over their lives.

When the Fourth Amendment was ratified, organized police forces did not exist.[58] Colonial policing was the "business of amateurs."[59] Sheriffs did not have a professional staff; they relied heavily on ordinary citizens to serve as constables or watchmen, whose primary duties consisted of patrolling rather than investigating.[60] The government typically became involved in criminal investigations only after an arrest was made or a suspect was identified, and in ordinary criminal cases, police rarely conducted searches prior to arrest.[61]

Organized police forces developed during the nineteenth century, and by the middle of the twentieth century, policing reached an unprecedented level of organization and coordination.[62] At the center of the rise of modern law enforcement was the development of the FBI. When the FBI was being formed in 1908, there was significant opposition in Congress to a permanent federal police force.[63] Members of Congress expressed trepidation over the possibility that such an in-

vestigatory agency could ascertain "matters of scandal and gossip" that could wind up being used for political purposes.[64] These concerns related to the potential dangers of the agency's information gathering capabilities, and as will be discussed later, the fears eventually became realities.

Today, we live in an endless matrix of law and regulation, administered by a multitude of vast government bureaucracies. Like most everything else in modern society, law enforcement has become bureaucratized. There are large police departments armed with sophisticated technology that coordinate with each other. There are massive agencies devoted entirely to investigation and intelligence gathering. One of the distinctive facets of law enforcement bureaucracy in the United States is that low-ranking officials exercise a profound degree of discretion, and most of their discretionary decisions are undocumented.[65]

Many factors make it difficult for law enforcement officials to strike a delicate balance between order and liberty. Among them, there are tremendous pressures on law enforcement agencies to capture criminals, solve notorious crimes, keep crime under control, and prevent acts of violence and terrorism. This highly stressful environment can lead to short cuts, bad exercises of discretion, or obliviousness and insensitivity to people's freedom. One of the most crucial aspects of keeping government power under control is a healthy scrutiny. Most law enforcement officials, however, are unlikely to view themselves with distrust and skepticism. Police and prosecutors are too enveloped in the tremendous responsibilities and pressures of their jobs to remain completely unbiased.

In short, one need not fear the rise of a totalitarian state or the inhibition of democratic activities to desire strong controls on the power of the government in collecting personal information. The Kafka metaphor more aptly captures what is harmful about these types of bureaucratic realities. The harm is that our personal data is stored within a bureaucratic system, where we are vulnerable to abuses, careless errors, and thoughtless decisions.

Leaks, Lapses, and Vulnerability. As more private-sector data becomes available to the government, there could be a de facto national

database, or a large database of "suspicious" individuals.[66] Federal governmental entities have engaged in extensive data gathering campaigns on various political groups throughout the twentieth century. From 1940 through 1973, for example, the FBI and CIA conducted a secret domestic intelligence operation, reading the mail of thousands of citizens. The FBI's investigations extended to members of the women's liberation movement and prominent critics of the Vietnam War, and the FBI obtained information about personal and sexual relationships that could be used to discredit them. During the McCarthy era and again in the 1980s, the FBI sought information from libraries about the reading habits of certain individuals. Between 1967 and 1970, the U.S. Army conducted wide-ranging surveillance, amassing extensive personal information about a broad group of individuals. The impetus for the Army's surveillance was a series of riots that followed Dr. Martin Luther King, Jr.'s assassination. The information collected involved data about finances, sexual activity, and health. In 1970, Congress significantly curtailed the Army's program, and the records of personal information were eventually destroyed.[67]

The danger of these information warehousing efforts is not only that it chills speech or threatens lawful protest, but also that it makes people more vulnerable by exposing them to potential future dangers such as leaks, security lapses, and improper arrests. For example, during the late 1960s and early 1970s, the Philadelphia Police Department (PPD) compiled about 18,000 files on various dissident individuals and groups. During a national television broadcast, PPD officials disclosed the names of some of the people on whom files were kept.[68]

Automated Investigations and Profiling. Government agencies are using personal information in databases to conduct automated investigations. In 1977, in order to detect fraud, the federal government began matching its computer employee records with those of people receiving federal benefits.[69] With the use of computers to match records of different government entities, the government investigated millions of people. Some matching programs used data obtained from merchants and marketers to discover tax, welfare, and food stamp fraud as well as to identify drug couriers.[70] This sharing of records between different government agencies, ordinarily a violation of the Privacy

Act, was justified under the "routine use" exception.[71] Computer matching raised significant concerns, and in 1988, Congress finally passed a law regulating this practice.[72] The law has been strongly criticized as providing scant substantive guidance and having little practical effect.[73]

This type of automated investigation is troubling because it alters the way that government investigations typically take place. Usually, the government has some form of particularized suspicion, a factual basis to believe that a particular person may be engaged in illegal conduct. Particularized suspicion keeps the government's profound investigative powers in check, preventing widespread surveillance and snooping into the lives and affairs of all citizens. Computer matches, Priscilla Regan contends, investigate everyone, and most people who are investigated are innocent.[74]

With the new information supplied by the private sector, there is an increased potential for more automated investigations, such as searches for all people who purchase books about particular topics or those who visit certain websites, or perhaps even people whose personal interests fit a profile for those likely to engage in certain forms of criminal activity. Profiles work similarly to the way that Amazon.com predicts which products customers will want to buy. They use particular characteristics and patterns of activity to predict how people will behave in the future. Of course, profiles can be mistaken, but they are often accurate enough to tempt people to rely on them. But there are even deeper problems with profiles beyond inaccuracies. Profiles can be based on stereotypes, race, or religion. A profile is only as good as its designer. Profiles are often kept secret, enabling prejudices and faulty assumptions to exist unchecked by the public. As Oscar Gandy observes, the use of profiling to form predictive models of human behavior incorrectly assumes that "the identity of the individual can be reduced, captured, or represented by measurable characteristics." Profiling is an "inherently conservative" technology because it "tends to reproduce and reinforce assessments and decisions made in the past."[75] Spiros Simitis explains that a profiled individual is "necessarily labeled and henceforth seen as a member of a group, the peculiar features of which are assumed to constitute her personal characteristics. Whoever appears in the lists

as a 'tax-evader,' 'assistance-chiseler,' or 'porno-film viewer' must be constantly aware of being addressed as such."[76]

Profiling or automated investigations based on information gathered through digital dossiers can result in targets being inappropriately singled out for more airport searches, police investigations, or even arrest or detention. Indeed, the federal government recently announced the creation of CAPPS II, the Computer Assisted Passenger Prescreening System, which employs computer databases to profile individuals to determine their threat level when flying. Based on their profiles, airline passengers are classified as green, yellow, or red. Passengers labeled green are subject to a normal security check; those in the yellow category receive additional searching; and those branded as red are not permitted to fly.[77] The government has not released details about what information is gathered, how people are profiled, whether race or nationality is a factor, or what ability, if any, people will have to challenge their classification.

People ensnared in the system face considerable hassle and delay. For example, in 2003, a 29-year-old member of the U.S. national rowing team was stopped at the gate when flying from Newark to Seattle. Although born in the United States, the young rower had a Muslim last name, which was probably a factor that led him to be placed on the no-fly list. When officials investigated, they cleared him, but it was too late—his flight had already left. This wasn't an isolated incident; it happened to him a few months earlier as well.[78] With no way to clear his name, he remains at risk of being detained, hassled, and delayed every time he goes to an airport.

Overreacting in Times of Crisis. The government can use dossiers of personal information in mass roundups of distrusted or suspicious individuals whenever the political climate is ripe. As legal scholar Pamela Samuelson observed: "One factor that enabled the Nazis to efficiently round up, transport, and seize assets of Jews (and others they viewed as 'undesirables') was the extensive repositories of personal data available not only from the public sector but also from private sector sources."[79] In the United States, information archives greatly assisted the roundups of disfavored groups, including Japanese Americans during World War II. Following the bombing of Pearl

Harbor on December 7, 1941, the FBI detained thousands of Japanese American community leaders in internment camps. These initial roundups were facilitated by an index of potentially subversive people of Japanese descent compiled by the Justice Department beginning in the late 1930s. In 1942, in the name of national security, about 120,000 people of Japanese descent living on the West Coast were imprisoned in internment camps. The Census Bureau prepared special tabulations of Japanese Americans, which assisted in the relocation.[80]

The acquisition of personal data also facilitated the Palmer Raids (or "Red Scare") of 1919–1920. A bomb blew up at the doorstep of Attorney General A. Mitchell Palmer's home.[81] Shortly thereafter, bombs went off in eight other cities. Letter bombs were mailed to many elites, but most were halted at the post office due to inadequate postage.[82] In a climate rife with fear of "Reds," anarchists, and labor unrest, Congress tasked the Bureau of Investigation (the organization that became the FBI in 1935) with addressing these terrorist threats.[83] Under the direction of a young J. Edgar Hoover, the Bureau of Investigation developed an extensive index of hundreds of thousands of radicals.[84] This data was used to conduct a massive series of raids, in which over 10,000 individuals suspected of being Communists were rounded up, many without warrants.[85] The raids resulted in a number of deportations, many based solely on membership in certain organizations.[86] When prominent figures in the legal community such as Roscoe Pound, Felix Frankfurter, and Zechariah Chafee, Jr., criticized the raids, Hoover began assembling a dossier on each of them.[87]

Additionally, personal information gathered by the FBI enabled the extensive hunt for Communists during the late 1940s and 1950s—a period of history that has since been criticized as a severe over-reaction, resulting in the mistreatment of numerous individuals, and impeding the reform agenda begun in the New Deal.[88] According to historian Ellen Schrecker, federal agencies' "bureaucratic interests, including the desire to present themselves as protecting the community against the threat of internal subversion, inspired them to exaggerate the danger of radicalism."[89] Senator Joseph R. McCarthy, the figure who epitomized the anti-Communism of the 1950s, received substantial assistance from Hoover, who secretly released information about suspected Communists to McCarthy.[90] Further, the FBI supplied a steady

stream of names of individuals to be called before the House Un-American Activities Committee (HUAC).[91] As historian Richard Powers observes, "information derived from the [FBI's] files was clearly the lifeblood of the Washington anti-communist establishment."[92] The FBI also leaked information about suspected individuals to employers and the press.[93] Public accusations of being a Communist carried an immense stigma and often resulted in a severe public backlash.[94] Individuals exposed as Communists faced retaliation in the private sector. Numerous journalists, professors, and entertainers were fired from their jobs and blacklisted from future employment.[95]

In short, government entities have demonstrated substantial abilities to gather and store personal information. Combined with the extensive data available about individuals in third party records, this creates a recipe for similar or greater government abuses in the future.

Changing Purposes and Uses. Information obtained by the government for one purpose can readily be used for another. For example, suppose the government is investigating whether a prominent critic of the war against terrorism has in any way assisted terrorists or is engaged in terrorism. In tracking an individual's activities, the government does not discover any criminal activity with regard to terrorism, but discovers that a popular website for downloading music files has been visited and that copyright laws have been violated. Such information may ultimately be used to prosecute copyright violations as a pretext for the government's distaste for the individual's political views and beliefs. Further, dossiers maintained by law enforcement organizations can be selectively leaked to attack critics.

Indeed, it is not far-fetched for government officials to amass data for use in silencing or attacking enemies, critics, undesirables, or radicals. For example, J. Edgar Hoover accumulated an extensive collection of files with detailed information about the private lives of numerous prominent individuals, including presidents, members of Congress, Supreme Court justices, celebrities, civil rights leaders, and attorney generals.[96] Hoover's data often included sexual activities.[97] Hoover used this information to blackmail people or to destroy their reputations by leaking it. Often, however, he did not even have to

make any explicit threats. Politicians—and even presidents—feared that Hoover had damaging information about them and would avoid criticizing Hoover or attempting to remove him as FBI director. Indeed, on one of the tapes President Nixon recorded in the Oval Office, he declared that he could not fire Hoover because Hoover knew too much information about him.[98]

We live in a world of mixed and changing motives. Data that is obtained for one purpose can be used for an entirely different purpose as motives change. For example, for several years, the FBI extensively wiretapped Martin Luther King, Jr.[99] They wiretapped his home, his office, and the hotel rooms that he stayed at when traveling.[100] Based on the wiretaps, the FBI learned of his extensive partying, extramarital affairs, and other sexual activities. A high-level FBI official even anonymously sent him a tape with highlights of the FBI's recordings, along with a letter that stated:

> King, there is only one thing left for you to do. You know what it is. You have just 34 days in which to do (this exact number has been selected for a specific reason, it has definite practical significant [*sic*]). You are done. There is but one way out for you. You better take it before your filthy, abnormal fraudulent self is bared to the nation.[101]

Hoover's motive is disputed. One theory is that King was wiretapped because he was friendly with a person who had previously been a member of the Communist Party.[102] Another theory is that Hoover despised King personally. Hoover's longstanding hatred of King is evidenced by his nasty public statements about King, such as calling King "the most notorious liar" in the nation.[103] This was probably due, in part, to King's criticism of the FBI for inadequately addressing the violence against blacks in the South, Hoover's overreaction to any criticism of the FBI, and the FBI's practice of consistently targeting its critics.[104] As David Garrow hypothesizes, the original reason that the FBI began collecting information about King was due to fears of Communist ties; however, this motivation changed once these fears proved unfounded and several powerful individuals at the FBI expressed distaste for King's sexual activities and moral behavior.[105]

Protecting Privacy with Architecture

The dangers discussed previously illustrate why privacy is integral to freedom in the modern state. As I discussed in chapter 6, we should move away from the invasion conception and seek to protect privacy through architectural solutions that regulate power in our various relationships. Protecting privacy through architecture differs from protecting it as an individual right. Viewing privacy as an individual right against government information gathering conceives of the harm to privacy as emanating from the invasion into the lives of particular people. But many of the people asserting a right to privacy against government information gathering are criminals or terrorists, people we do not have a strong desire to protect. In modern Fourth Amendment law, privacy protection is often initiated at the behest of specific individuals, typically those accused of crimes. Often these individuals' rights conflict with the need for effective law enforcement and the protection of society. Why should one individual's preference for privacy trump the social goals of security and safety? This question is difficult to answer if privacy is understood as a right possessed by particular people.

In contrast, architecture protects privacy differently and is based on a different conception of privacy. Privacy is not merely a right possessed by individuals, but is a form of freedom built into the social structure. It is thus an issue about the common good as much as it is about individual rights. It is an issue about social architecture, about the relationships that form the structure of our society.

One might dismiss the abuses of government information gathering as caused by a few rogue officials. But according to David Garrow, the FBI that targeted Martin Luther King, Jr. was not a "deviant institution in American society, but actually a most representative and faithful one."[106] In other words, the FBI reflected the mindset of many Americans, embodying all the flaws of that mindset. We like to blame individuals, and certainly the particular abusers are worthy of admonition, but we cannot overlook the fact that the causes of abuse often run deeper than the corrupt official. Abuse is made possible by a bureaucratic machinery that is readily susceptible to manipulation. Thus, the problem lies in institutional structures and architectures of

power. In the latter half of the twentieth century, and continuing to the present, one of the aspects of this architecture has been the lack of control over government information gathering.

What is the most effective architecture to structure the way that the government can access personal information held by third parties? In the next chapter, I discuss two architectures, that of the Fourth Amendment, which the Court has concluded doesn't apply to data held by third parties, and that of the statutory regime which has arisen in its place.