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: 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 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 \textit{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

Notes 229
Index 267
About the Author 283
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.
From the beginning of the twentieth century, we have witnessed a vast proliferation in the number of government records kept about individuals as well as a significant increase in public access to these records. These trends together have created a problematic state of affairs—a system where the government extracts personal information from the populace and places it in the public domain, where it is hoarded by private-sector corporations that assemble dossiers on almost every American citizen.

**Records from Birth to Death**

Today, federal, state, and local government entities maintain a smorgasbord of public records.\(^1\) State public records cover one's life from birth to death. Birth records can contain one's name, date of birth, place of birth, full names and ages of one's parents, and mother's maiden name.\(^2\) In particular, mother's maiden names are important because many companies use them as passwords to access more sensitive data. Shortly after birth, the federal government stamps an
individual with a SSN, which will be used throughout her life to identify her and consolidate records about her. States also maintain other records relating to one’s personal life, such as records about marriages, divorces, and death. These are often referred to collectively as “vital records.” Records of marriages, which are public in most states, contain maiden names, the date and place of birth of both spouses, as well as their residential addresses.

Beyond vital records, states keep records for almost every occasion an individual comes into contact with the state bureaucracy. Accident reports and traffic citation records are made publicly available by many states. Voting records can reveal one’s political party affiliation, date of birth, place of birth, email address, home address, telephone number, and sometimes SSN. In many states, this information is publicly available.

An individual’s profession and place of employment often generate a number of records. Many professions require licenses, such as doctors, lawyers, engineers, insurance agents, nurses, police, accountants, and teachers. If an individual is injured at work, worker’s compensation records may disclose the date of birth, type of injury, and SSN. If a person is a public employee, many personal details are released to the public by way of personnel records, including home address, phone number, SSN, salary, sick leave, and sometimes even email messages. In Massachusetts, government officials are required by law to maintain “street lists” containing the names, addresses, dates of birth, veteran statuses, nationalities, and occupations of all residents. These lists, which organize residents by the streets they live on, are made available to the police, to all political committees and candidates, and to businesses and other organizations.

One’s home and property are also a matter of public record. Property tax assessment records contain a detailed description of the home, including number of bedrooms and bathrooms, amenities such as swimming pools, the size of the house, and the value. Other property ownership records unveil lifestyle information such as whether one owns a boat, and if so, its size and type.

Often, any contact with law enforcement officials will yield a record. Arrest records can include a person’s name, occupation, physical description, date of birth, and the asserted factual circumstances.
surrounding the arrest. Police records also contain information about victims of crime.

Court records can be very revealing. In almost all states, court records are presumed to be public. Although current practice and existing physical constraints limit the extent to which personal information in court documents can be accessed, new technologies are on the verge of changing this reality.

In civil cases, court files may contain medical histories, mental health data, tax returns, and financial information. For example, in an ordinary civil lawsuit over an automobile accident, the plaintiff must submit medical information, including any pre-existing conditions that might be responsible for her symptoms. This data could even include psychological information. To establish damages, the plaintiff must also reveal details about her lifestyle, activities, and employment. If this information is contained in a document filed with the court or is mentioned in a hearing or at trial, it can potentially become accessible to the public unless protected by a protective order. In addition to plaintiffs, civil defendants must also yield personal information in many instances.

Witnesses and other third parties who are involved in cases can have deeply personal details snared by discovery and later exposed in court documents. If a person serves as a juror, her name, address, spouse’s name, occupation, place of employment, and answers to voir dire questions may become part of the court record. Some courts have held that the public may have access to questionnaires given to jurors as part of voir dire. Voir dire questions can involve sensitive matters such as whether a juror was the victim of a crime, the juror’s political and religious beliefs, any medical and psychological conditions that might affect the juror’s performance, and other private details.

Beyond ordinary civil lawsuits, special civil proceedings, such as appeals from the denial of Social Security benefits, release much information into court records, including a person’s disability, work performance, SSN, birth date, address, phone number, and medical records. In federal bankruptcy courts, any “paper filed . . . and the dockets of a bankruptcy court are public records and open to examination by an entity at reasonable times without charge.” Information
involved in bankruptcy proceedings includes one’s SSN, account numbers, employment data, sources of income, expenses, debts owed, and other financial information. Additionally, in certain circumstances, employees of a company that declares bankruptcy can have their personal information divulged in public bankruptcy records.

In some states, family court proceedings are public. For example, a divorce proceeding can unmask the intimacies of marital relationships. As the New Hampshire Supreme Court held, “[a] private citizen seeking a divorce in this State must unavoidably do so in a public forum, and consequently many private family and marital matters become public.”

Parties in criminal cases have even less privacy. Beyond the personal details about a defendant released at trial or in the government’s indictment or charging papers, conviction records are made public. Information about victims—their lifestyles, medical data, and occupation—can also be found in court records. Pre-sentence reports prepared by probation officers about convicted defendants facing sentence are used by judges in arriving at the appropriate sentence. These reports contain a summary of the defendant’s prior criminal conduct, social history, character, family environment, education, employment and income, and medical and psychological information. Although in many states and in federal court, pre-sentence reports remain confidential, in some states, such as California, the pre-sentence report becomes part of the court file after sentencing.

Community notification laws for sex offenders, often referred to as “Megan’s Laws,” require the maintenance of databases of information about prior sex offenders and disclosure of their identities and where they live. All 50 states have enacted some version of Megan’s Law. Sex offender records often contain SSNs, photographs, addresses, prior convictions, and places of employment. A number of states have placed their sex offender records on the Internet.

Some localities are even publicizing records about individuals arrested, but not yet convicted, of certain crimes. In 1997 Kansas City initiated “John TV,” broadcasting on a government-owned television station the names, photographs, addresses, and ages of people who
had merely been arrested (not convicted) for soliciting prostitutes, and other cities have initiated similar programs. Additionally, a growing number of states are furnishing online databases of all of their current inmates and parolees.

The Impact of Technology

For a long time, public records have been accessible only in the various localities in which they were kept. A person or entity desiring to find out about the value of an individual’s home would have to travel to the town or county where the property was located and search through the records at the local courthouse. Depending upon local practice, the seeker of a record might be able to obtain a copy through the mail. Court records, such as bankruptcy records, would typically be obtained by visiting a courthouse or engaging in a lengthy correspondence with the clerk’s office. The seeker of a record could not obtain records en masse; records could only be obtained for specific individuals.

This reality is rapidly changing. As records are increasingly computerized, entire record systems rather than individual records can be easily searched, copied, and transferred. Private-sector organizations sweep up millions of records from record systems throughout the country and consolidate them into gigantic record systems. Many websites now compile public records from across the country. There are more than 165 companies offering public record information over the Internet. These companies have constructed gigantic databases of public records that were once dispersed throughout different agencies, offices, and courthouses—and with the click of a mouse, millions of records can be scoured for details.

The increasing digitization of documents and the use of electronic filing will soon result in much greater accessibility to court records online. Currently, most courts post only court rulings and schedules on their websites. Only a handful of courts now post complaints and other legal documents. However, states are beginning to require documents to be filed electronically and to convert existing records into digital format. For example, in New Jersey, bankruptcy records (including a debtor’s bankruptcy petition) are scanned into electronic...
format and can be accessed through the Internet. Some companies are beginning to make digital images of records available over the Internet. The federal court system is currently developing a system that makes full case files accessible via the Internet.

Beyond greater accessibility, technology may also lead to the retention of greater amounts of personal information in public records. Under current practice, due to storage space constraints, clerks’ offices often do not maintain copies of exhibits and other documents related to trials. However, as court documents such as pleadings and exhibits are filed in digital format, they will become easier to store. Further, under current practice, transcripts are typically produced only when a case is appealed. New technology enables transcripts of court proceedings to be made instantaneously without having to be transcribed. The increased use of such technology could result in the existence of more transcripts of trials, which can potentially include personal information about many parties and witnesses.

In sum, the increasing digitization of documents enables more documents to be retained by eliminating storage constraints, increases the ability to access and copy documents, and permits the transfer of documents en masse. Personal information in public records, once protected by the practical difficulties of gaining access to the records, is increasingly less obscure.

**The Regulation of Public Records**

As it currently stands, public records law is a complicated and diverse hodge-podge of various statutes, court practices, and common law rights that vary from state to state and leave much personal information unprotected. A broad overview of the law that governs public records reveals that it is disconnected, often outdated, and inadequate to meet the challenges of the new technologies of the Information Age.

*The Common Law, Court Records, and Protective Orders.* At common law, English courts rarely encountered cases involving an individual seeking to gain access to government records. Only in unusual circumstances could individuals inspect government records, such as when
people needed them for court proceedings. Access to court records, as opposed to other public records, was broader. When documents were introduced into evidence, individuals were permitted access.

Early U.S. courts followed the English practice. Only if a person had a “special interest” in examining records would access be granted. Later on, the common law evolved to expand the “interest” required for inspection to include redressing public wrongs and monitoring government functions. The law then broadened even further to include all purposes that were not improper or harmful to others. One of the most commonly mentioned improper purposes was “to satisfy idle curiosity or for the purpose of creating a public scandal.”

In contrast to public records, the right to inspect court records was generally broader and was shaped by the supervisory authority of the courts. The courts had a long tradition of permitting open access to court records, and access was rarely limited based on the purposes for which the records were sought. In 1978, in Nixon v. Warner Communications, Inc., the Supreme Court noted that “[i]t is clear that the courts of this country recognize a general right to inspect and copy public records and documents, including judicial records and documents.” The right is justified by “the citizen’s desire to keep a watchful eye on the workings of public agencies, and in a newspaper publisher’s intention to publish information concerning the operation of government.” The common law right of access isn’t absolute, especially for court records, because “[e]very court has supervisory power over its own records and files,” and can deny access when records reveal embarrassing personal information or cause harm. The decision over whether to permit access “is one best left to the sound discretion of the trial court.”

In the federal court system, pursuant to Federal Rule of Civil Procedure 26(c), judges have discretion “for good cause shown” to issue protective orders to shield information from disclosure where it might cause a party “annoyance, embarrassment, oppression, or undue burden or expense.” Protective orders allow documents to be used by parties to a case, but restrict public access. Most states have a rule similar to Rule 26(c). Since court records are presumed to be publicly accessible, a party seeking a protective order must overcome the presumption. Courts balance a party’s interest in privacy against
the public interest in disclosure. If a court decides to deny access, it “must set forth substantial reasons.”

Courts also retain discretion to issue special orders to keep certain proceedings and information confidential. A court will sometimes, under very limited circumstances, seal court proceedings such as trials. A court can allow a plaintiff to proceed anonymously with the use of a pseudonym. Courts can also permit anonymous juries when jurors might otherwise be placed in danger. These decisions, however, are within the discretion of the trial court, and courts differ greatly in the exercise of their discretion. For example, one court permitted a woman who had been raped at a train station and was suing Amtrak to keep her identity secret because of the potential embarrassment she would suffer if the details of her rape became known in her community. In contrast, another court held that a victim of sexual assault could not sue her assailant for civil damages under a pseudonym because “[f]airness requires that she be prepared to stand behind her charges publicly” and because she was “seeking to vindicate primarily her own interests.”

In sum, under modern American common law, there is a limited right to access public records so long as one’s purpose is not improper. For court records, the common law right to access follows the supervisory authority of the courts, and judges have significant discretion in granting or denying access.

*Freedom of Information Laws.* State legislatures gradually replaced or supplemented the common law right of access with open records statutes, which generally mandated broad access. These statutes are called “freedom of information,” “open access,” “right to know,” or “sunshine” laws. States were initially slow in enacting statutory public access rights; by 1940, only 12 states had open records statutes. In 1966, Congress passed the Freedom of Information Act (FOIA), providing substantial public access to records of the federal government. When he signed the FOIA into law, President Lyndon Johnson declared that “democracy works best when the people have all the information that the security of the Nation permits. No one should be able to pull curtains of secrecy around decisions which can be revealed without injury to the public interest.” Under FOIA, “any person” (in-
cluding associations, organizations, and foreign citizens) may request “records” maintained by an executive agency. Requesters of records don’t need to state a reason for requesting records. FOIA does not apply to records kept by Congress or the Judiciary.

Today, all 50 states have open records statutes, a majority of which are modeled after the FOIA. Like the federal FOIA, state FOIAs are justified by a strong commitment to openness and transparency. Following FOIA, many states eliminated the common law requirement that requesters establish an interest in obtaining the records. Most state FOIAs contain a presumption in favor of disclosure.

Open access laws never mandate absolute disclosure. They contain exemptions, typically (although not always) including an exemption to protect individual privacy. The federal FOIA contains nine enumerated exemptions to disclosure, two of which pertain to privacy. One applies generally to records which “would constitute a clearly unwarranted invasion of personal privacy”; the other applies to law enforcement records that could “constitute an unwarranted invasion of personal privacy.” If possible, private information can be deleted from records, and the redacted records disclosed to the requester.

The federal FOIA doesn’t require that a person be given notice that his or her personal information is encompassed within a FOIA request. Even if an individual finds out about the request, she has no right under FOIA to prevent or second-guess an agency’s decision to disclose the records. FOIA does not require that the government withhold information; it is up to the government agency to assert and to litigate the individual’s privacy interest.

State FOIA privacy exemptions come in myriad shapes and sizes. Many state FOIAs contain privacy exemptions similar to those found in the federal FOIA, applying when disclosure would constitute a “clearly unwarranted” invasion of privacy. However, not all state FOIAs have privacy exemptions. Pennsylvania’s Right to Know Act does not contain a privacy exemption; it prohibits only access to records “which would operate to the prejudice or impairment of a person’s reputation or personal security.” As one court stated, “the phrase ‘personal security’ does not mean ‘personal privacy.’” Ohio’s Public Records Act does not contain any privacy exemption.
In applying FOIA privacy exemptions, many states follow the federal FOIA approach and balance interests of privacy against the interests of public access. However, states have adopted widely differing approaches often stemming from vastly different judicial conceptions of privacy.

**Privacy Acts.** The Privacy Act of 1974 regulates the record systems of federal agencies. The Act prohibits the disclosure of personal information; requires records to be kept secure; and gives people the right to review their records and to ask the agency to correct any errors. People can sue if they are harmed by an agency’s failure to comply with the Act. The Privacy Act has significant limitations. It is limited only to the public sector. It applies to federal, not state and local agencies. Further, the Act has been eroded by about a dozen exceptions. For example, agencies can disclose information without the consent of individuals to the Census Bureau, to law enforcement entities, to Congress, and to credit reporting agencies. When FOIA requires that information be released, the Privacy Act does not apply. Nor does the Privacy Act apply to court records.

The broadest exception is that information may be disclosed for any “routine use” if disclosure is “compatible” with the purpose for which the agency collected the information. The “routine use” exception has repeatedly been criticized as being a gigantic loophole. As privacy law expert Robert Gellman writes, “[t]his vague formula has not created much of a substantive barrier to external disclosure of personal information.”

Although the Privacy Act requires an individual’s permission before his or her records can be disclosed, redress for violations of the Act is virtually impossible to obtain. The Privacy Act provides individuals with a monetary remedy for disclosures of personal information only if the disclosure was made “willfully and intentionally.” This restriction on recovery of damages fails to redress the most common form of mistakes—those due to carelessness. This leaves little incentive to bring suit against violators. For example, in *Andrews v. Veterans Administration*, the Veterans Administration released inadequately redacted personnel records of nurses, resulting in what the
court called a “substantial” violation of nurses’ privacy. However, the agency could not be sued under the Privacy Act because it acted negligently, not willfully. Moreover, less than a third of the states have enacted a general privacy law akin to the Privacy Act. Paul Schwartz observes that most states lack “omnibus data protection laws” and have “scattered laws [that] provide only limited protections for personal information in the public sector.”

Access and Use Restrictions. Confronted with increased information trade, some states have attempted to restrict access to personal information in public records as well as certain uses of personal information obtained from public records. In the last decade, a number of states have enacted access restrictions for some of their public records, often excluding access for commercial uses, such as soliciting business or marketing services or products. For example, Georgia amended its public records law in 1991, making it unlawful to access law enforcement or motor vehicle accident records “for any commercial solicitation of such individuals or relatives of such individuals.” In 1992, Louisiana restricted access to accident records for commercial solicitation purposes. Kentucky, in response to “a public groundswell [that] developed against the release of accident reports to attorneys and chiropractors,” amended its public records law in 1994 to restrict access for these and other commercial uses. In 1996, Florida barred the access of driver information in traffic citations from those seeking it for commercial solicitation purposes. Colorado curtailed access to criminal justice records unless those seeking access signed a statement that such records would not be used “for the direct solicitation of business for pecuniary gain.” California restricted access to arrest records by providing that the records “shall not be used directly or indirectly to sell a product or service . . . and the requester shall execute a declaration to that effect under penalty of perjury.” Almost half of the states prohibit the commercial use of voter registration records.

The federal government also has certain access and use restrictions for its public records. Pursuant to the Federal Election Campaign Act (FECA), reports of contributors to political committees are
“available for public inspection . . . except that any information copied from such reports . . . may not be sold or used by any person for the purpose of soliciting contributions or for commercial purposes.”

In sum, although in certain contexts laws are beginning to limit access to public records for some purposes, the vast majority of public records remain virtually unrestricted in access.

Restrictions on State Information Practices. In a rare instance, the federal government has directly regulated the states’ use of public records. In 1994, Congress passed the Driver’s Privacy Protection Act (DPPA) to curtail states’ selling their motor vehicle records to marketers. In Reno v. Condon, the Supreme Court concluded that DPPA was a proper exercise of Congress’s authority to regulate interstate commerce. Further, the Court concluded that DPPA “regulates the States as the owners of databases” and does not require them to enact regulation or to assist in enforcing federal statutes concerning private individuals. Although DPPA is an important first step in bringing state public records systems under control, DPPA applies only to motor vehicle records and does not forbid the dissemination of all the other public records states maintain.

The Regulatory Regime of Public Records. As illustrated throughout this chapter, states vary significantly in what information they make publicly available. Often such decisions are made by agencies and bureaucrats or left to the discretion of the courts. Decisions as to the scope of access—whether one must obtain a record by physically going to a local agency office, by engaging in correspondence by mail, or by simply downloading it from the Internet—are often made by local bureaucrats. Frequently, it is up to the individual to take significant steps to protect privacy, such as overcoming the presumption of access to court records. In many instances, individuals are never even given notice or an opportunity to assert a privacy interest when records containing their personal information are disclosed.

Differing protection of personal information with no minimum floor of protection presents significant problems in today’s age of increasing mobility and information flow. There is no federal law estab-
lishing a baseline for the regulation of public records. Thus, personal information is regulated by a bewildering assortment of state statutory protections, which vary widely from state to state.97

This chaotic state of affairs is troublesome in an Information Age where information so fluidly passes throughout the country and is being made more widely available through the Internet. The privacy protection that currently exists for public records is largely designed for a world of paper records and has been slow to adapt to an age where information can be downloaded from the Internet in an instant.