

the digital person

TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE



daniel j. solove

the
digital
person

010

1 0 1 0 1 0 1 0 1 0 1 0 1
1 0 1 0 1 0 1 0 1 0 1
1 0 1 0 1 0 1 0 1
1 0 1 0 1 0 1
1 0 1 0 1
1 0 1
1

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

© 2004 by New York University

All rights reserved

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

0
1 0
0 1 0
1 0 1 0
0 1 0 1 0
1 0 1 0 1 0
0 1 0 1 0 1 0
1 0 1 0 1 0
0 1 0 1 0
1 0 1 0
0 1 0
1 0
0

*In loving memory of
my grandma,
Jean*

Contents

Acknowledgments	ix
I Introduction	1
The Problems of Digital Dossiers	2
Traditional Conceptions of Privacy	7
Rethinking Privacy	8
A Road Map for This Book	9

i computer databases

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 public records

7 The Problem of Public Records	127
Records from Birth to Death	127

The Impact of Technology	131
The Regulation of Public Records	132

8 Access and Aggregation:

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

iii government access

9 Government Information Gathering 165

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

10 The Fourth Amendment, Records, and Privacy 188

The Architecture of the Fourth Amendment	188
The Shifting Paradigms of Fourth Amendment Privacy	195
The New <i>Olmstead</i>	200
The Emerging Statutory Regime and Its Limits	202

11 Reconstructing the Architecture 210

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

12 Conclusion	223
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 Ringer, 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.

4 The Problems of Information Privacy Law

A distinctive domain of law relating to information privacy has been developing throughout the twentieth century. Although the law has made great strides in dealing with privacy problems, the law of information privacy has been severely hampered by the difficulties in formulating a compelling theory of privacy. The story of privacy law is a tale of changing technology and the law's struggle to respond in effective ways.

Information privacy law consists of a mosaic of various types of law: tort law, constitutional law, federal and state statutory law, evidentiary privileges, property law, and contract law. Much of privacy law is interrelated, and as legal scholar Ken Gormley observes, "various offshoots of privacy are deeply intertwined at the roots, owing their origins to the same soil."¹

Information privacy law has made great strides toward protecting privacy. Nevertheless, there are systematic deficiencies across the spectrum of privacy law in addressing the special nature of the problem of digital dossiers.

The Privacy Torts

Warren and Brandeis. Privacy law owes its greatest debt to Samuel Warren and Louis Brandeis. Warren and Brandeis practiced law together in a Boston law firm. Brandeis later went on to become a Supreme Court justice.² In 1890, they wrote their profoundly influential article, *The Right to Privacy*,³ considered by many to be one of the primary foundations of privacy law in the United States.⁴ In the article, Warren and Brandeis raised alarm at the intersection of yellow journalism,⁵ with its increasing hunger for sensational human interest stories, and the development of new technologies in photography. During the latter half of the nineteenth century, newspapers were the most rapidly growing form of media, with circulation increasing about 1,000 percent from 1850 to 1890. In 1850, there were approximately 100 newspapers with 800,000 readers. By 1890, there were 900 papers with over 8 million readers. This massive growth was due, in part, to yellow journalism, a form of sensationalistic reporting that focused on scandals and petty crimes. Reaping the successes of yellow journalism, Joseph Pulitzer and William Randolph Hearst became the barons of the newspaper business. According to Warren and Brandeis: “The press is overstepping in every direction the obvious bounds of propriety and decency. Gossip is no longer the resource of the idle and of the vicious, but has become a trade, which is pursued with industry as well as effrontery.”⁶

Warren and Brandeis also expressed concern over what they called “instantaneous” photography. Although photography had been around before 1890, recent developments made photography much cheaper and easier. Cameras had been large, expensive, and not readily portable. In 1884, the Eastman Kodak Company came out with the “snap camera,” a hand-held camera for the general public. For the first time, people could take candid photographs. Warren and Brandeis feared the intersection of this new photographic technology with the gossip-hungry press: “Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that ‘what is whispered in the closet shall be proclaimed from the house-tops.’”⁷

On the surface, observed Warren and Brandeis, the existing common law failed to afford a remedy for privacy invasions. But it contained the seeds to develop the proper protection of privacy. The authors looked to existing legal rights and concluded that they were manifestations of a deeper principle lodged in the common law—“the more general right of the individual to be let alone.”⁸ From this principle, new remedies to protect privacy could be derived. Warren and Brandeis suggested that the primary way to safeguard privacy was through tort actions to allow people to sue others for privacy invasions.

What Warren and Brandeis achieved was nothing short of magnificent. By pulling together various isolated strands of the common law, the authors demonstrated that creating remedies for privacy invasions wouldn’t radically change the law but would merely be an expansion of what was already germinating.

As early as 1903, courts and legislatures responded to the Warren and Brandeis article by creating a number of privacy torts to redress the harms that Warren and Brandeis had noted.⁹ These torts permit people to sue others for privacy violations. In 1960, William Prosser, one of the most renowned experts on tort law, surveyed over 300 privacy cases in the 70 years since the publication of the Warren and Brandeis article.¹⁰ He concluded that the cases could be classified as involving four distinct torts.¹¹ These torts are: (1) intrusion upon seclusion; (2) public disclosure of private facts; (3) false light; and (4) appropriation. Today, whether by statute or common law, most states recognize some or all of the privacy torts.¹²

The privacy torts emerged in response to the privacy problems raised by Warren and Brandeis—namely, the incursions into privacy by the burgeoning print media. Today, we are experiencing the rapid rise of a new form of media—the Internet. Although the press still poses a threat to privacy, and photography has become an indispensable tool of journalism (as Warren and Brandeis accurately predicted), there are now many additional threats to privacy other than the press. The privacy torts are capable of redressing specific harms done to individuals—such as when the press discloses a deeply embarrassing secret about a private figure—but are not well adapted to

regulating the flow of personal information in computer databases and cyberspace.

Intrusion upon Seclusion. The tort of intrusion upon seclusion protects against the intentional intrusion into one's "solitude or seclusion" or "private affairs or concerns" that "would be highly offensive to a reasonable person."¹³ Although this tort could be applied to the information collection techniques of databases, most of the information collection is not "highly offensive to a reasonable person." Each particular instance of collection is often small and innocuous; the danger is created by the aggregation of information, a state of affairs typically created by hundreds of actors over a long period of time. Indeed, courts have thrown out cases for intrusion involving the type of information that would likely be collected in databases. For example, courts have rejected intrusion actions based on obtaining a person's unlisted phone number, selling the names of magazine subscribers to direct mail companies, and collecting and disclosing an individual's past insurance history.¹⁴ Further, intrusion must involve an invasion of "seclusion," and courts have dismissed intrusion suits when plaintiffs have been in public places. With regard to databases, much information collection and use occurs in public, and indeed, many parts of cyberspace may well be considered public places. Therefore, the tort of intrusion cannot provide an adequate safeguard against the gathering of personal information for databases.

Public Disclosure of Private Facts. The tort of public disclosure of private facts creates a cause of action when one makes public "a matter concerning the private life of another" in a way that "(a) would be highly offensive to a reasonable person, and (b) is not of legitimate concern to the public."¹⁵ Courts have sustained public disclosure suits for printing a photograph of a woman whose dress was blown up involuntarily by air jets; for publishing an article describing an individual's unusual disease; and for posting a large sign in a window stating that a person owed a debt.¹⁶

Although this tort could conceivably be applied to certain uses of databases, such as the sale of personal information by the database

industry, the tort of private facts appears to be designed to redress excesses of the press, and is accordingly focused on the widespread dissemination of personal information in ways that become known to the plaintiff. In contrast, databases of personal information are often transferred between specific companies, not broadcast on the evening news. Even if marketers disclosed information widely to the public, the tort is limited to “highly offensive” facts, and most facts in databases would not be highly offensive if made public. Moreover, some marketing data may already be in a public record, or by furnishing data in the first place, an individual may be deemed to have assented to its dissemination.

Additionally, the disclosure of personal information through the use and sale of databases is often done in secret. The trade in information is done behind closed doors in a kind of underworld that most people know little about. This secret trading of data is often completely legal. Thus, it would be difficult for a plaintiff to discover that such sales or disclosures have been made. Even if people are generally aware that their data is being transferred, they will often not be able to find out the specifics—what companies are receiving it and what these companies plan to do with it. As a result, the public disclosure tort is not well-adapted to combating the flow of personal information between various companies.

False Light. The tort of false light is primarily a variation on the defamation torts of libel and slander, protecting against the giving of “publicity to a matter concerning another that places the other before the public in a false light” that is “highly offensive to a reasonable person.”¹⁷ Like defamation, this tort has limited applicability to the types of privacy harms created by the collection and use of personal information by way of computer databases. Both defamation and false light protect one’s reputation, but the type of information collected in databases often is not harmful to one’s reputation.

Appropriation. The tort of appropriation occurs when one “appropriates to his own use or benefit the name or likeness of another.”¹⁸ In the courts, this tort has developed into a form of intellectual property right in aspects of one’s personhood. The interest protected is the in-

dividual's right to "the exclusive use of his own identity, in so far as it is represented by his name or likeness."¹⁹ For example, people can sue under this tort when their names or images are used to promote a product without their consent.²⁰

Appropriation could be applied to database marketing, which can be viewed as the use of personal information for profit. However, the tort's focus on protecting the commercial value of personal information has often prevented it from being an effective tool in grappling with the database privacy problem. In *Dwyer v. American Express Co.*, a court held there was no appropriation when American Express sold its cardholders' names to merchants because "an individual name has value only when it is associated with one of defendants' lists. Defendants create value by categorizing and aggregating these names. Furthermore, defendants' practices do not deprive any of the cardholders of any value their individual names may possess."²¹ In *Shibley v. Time, Inc.*, a court held that there was no action for appropriation when magazines sold subscription lists to direct mail companies because the plaintiff was not being used to endorse any product.²² The appropriation tort often aims at protecting one's economic interest in a form of property, and it is most effective at protecting celebrities who have created value in their personalities. This is not the same interest involved with privacy, which can be implicated regardless of the economic value accorded to one's name or likeness.

An Overarching Problem. Even if it were possible to eliminate the above difficulties with some minor adjustments to the privacy torts, the privacy problem with databases transcends the specific injuries and harms that the privacy torts are designed to redress. By its nature, tort law looks to isolated acts, to particular infringements and wrongs. The problem with databases does not stem from any specific act, but is a systemic issue of power caused by the combination of relatively small actions, each of which when viewed in isolation would appear quite innocuous. Many modern privacy problems are the product of information flows, which occur between a variety of different entities. There is often no single wrongdoer; responsibility is spread among a multitude of actors, with a vast array of motives and aims, each doing

different things at different times. For example, when a person unwittingly finds herself embroiled in a public news story, the invasiveness of the media is often not the product of one particular reporter. Rather, the collective actions of numerous reporters camping outside a person's home and following her wherever she goes severely disrupt her life. The difficulty in obtaining a legal remedy for this disruption is that no one reporter's actions may be all that invasive or objectionable. The harm is created by the totality of privacy invasions, but the tort of intrusion upon seclusion only focuses on each particular actor.²³

In sum, tort law often views privacy invasions separately and individually; but the problems of digital dossiers emerge from the collective effects of information transactions, combinations, lapses in security, disclosures, and abusive uses. Therefore, solutions involving the retooling of tort law will be severely limited in redressing the problem.

Constitutional Law

The U.S. Constitution protects privacy in a number of ways even though the word "privacy" does not appear in the document. Although the Constitution does not explicitly provide for a right to privacy, a number of its provisions protect certain dimensions of privacy, and the Supreme Court has sculpted a right to privacy by molding together a variety of constitutional protections. Beyond the U.S. Constitution, many states protect privacy in their own constitutions—some with an explicit right to privacy.²⁴

The U.S. Constitution only protects against state action, and many databases belong to the private sector. However, since the government is often a supplier of information to the private sector and is a major source of databases, constitutional protection could serve as a good potential tool for grappling with the problem.

The First Amendment. In addition to protecting free speech, the First Amendment safeguards the right of people to associate with one another. Freedom of association restricts the government's ability to demand organizations to disclose the names and addresses of their

members or to compel people to list the organizations to which they belong.²⁵ As the Supreme Court reasoned, privacy is essential to the freedom to associate, for it enables people to join together without having to fear loss of employment, community shunning, and other social reprisals.²⁶ However, privacy of associations is becoming more difficult in a world where online postings are archived, where a list of the people a person contacts can easily be generated from telephone and email records, and where records reveal where a person travels, what websites she visits, and so on. The Supreme Court has repeatedly held that the First Amendment protects anonymous speech, and it can restrict the government from requiring the disclosure of information that reveals a speaker's identity.²⁷ However, the First Amendment only applies when the government plays a role in the compulsion of the information,²⁸ and most of the gathering of personal information by companies isn't done under the pressure of any law.

The Fourth and Fifth Amendments. The Fourth Amendment restricts the government from conducting “unreasonable searches and seizures.”²⁹ It typically requires that government officials first obtain judicial authorization before conducting a search. According to the Supreme Court, “[t]he overriding function of the Fourth Amendment is to protect personal privacy and dignity against unwarranted intrusion by the State.”³⁰ The Fifth Amendment provides for a privilege against self-incrimination.³¹ The government cannot compel individuals to disclose incriminating information about themselves. In 1886, the Court articulated how the Fourth and Fifth Amendments worked in tandem to protect privacy. The case was *Boyd v. United States*.³² The government sought to compel a merchant to produce documents for use in a civil forfeiture proceeding. The Court held that the government could not require the disclosure of the documents because “any forcible and compulsory extortion of a man's own testimony or of his private papers to be used as evidence to convict him of crime or to forfeit his goods” is an “invasion of his indefeasible right to personal security, personal liberty and private property.”³³

As the administrative state blossomed throughout the twentieth century, the Court sidestepped the broad implications of *Boyd*. The administrative state spawned hundreds of agencies and a vast

bureaucracy that maintained records of personal information. As William Stuntz notes, “[g]overnment regulation required lots of information, and *Boyd* came dangerously close to giving regulated actors a blanket entitlement to nondisclosure. It is hard to see how modern health, safety, environmental, or economic regulation would be possible in such a regime.”³⁴ Therefore, the Court abandoned *Boyd*, and it increasingly curtailed the Fourth and Fifth Amendments from regulating the burgeoning government record systems.³⁵

The Fourth and Fifth Amendments protect only against government infringements, and do nothing to control the collection and use of information by private bureaucracies. Although it does not apply to the private sector, the Fourth Amendment does have the potential to protect against one problem with digital dossiers. The rise of digital dossiers in the private sector is becoming of increasing interest to law enforcement officials. I will discuss this issue in great depth in part III of this book. As I will demonstrate, the secrecy paradigm has made the Fourth Amendment practically inapplicable when the government seeks to tap into private-sector dossiers. In *Smith v. Maryland*,³⁶ the Court held that there was no reasonable expectation of privacy in the phone numbers one dials. The Court reasoned that such phone numbers were not secret because they were turned over to third parties (phone companies).³⁷ Similarly, in *United States v. Miller*, the Court held that financial records possessed by third parties are not private under the Fourth Amendment.³⁸ The Court’s focus—which stems from the paradigm that privacy is about protecting one’s hidden world—leads it to the view that when a third party has access to one’s personal information, there can be no expectation of privacy in that information.

The Right to Privacy. Beyond specific constitutional provisions, the Supreme Court has held that the Constitution implicitly protects privacy. In 1965, in *Griswold v. Connecticut*, the Court held that a state could not ban the use of or counseling about contraceptives because it invaded the “zone of privacy” protected by the Constitution.³⁹ Although there is no part of the Bill of Rights that directly establishes a right to privacy, such a right is created by the “penumbras” of many of the 10 amendments that form the Bill of

Rights. In *Roe v. Wade*, the Court held that the right to privacy “is broad enough to encompass a woman’s decision whether or not to terminate her pregnancy.”⁴⁰

In the 1977 decision, *Whalen v. Roe*, the Supreme Court extended substantive due process privacy protection to information privacy. New York passed a law requiring that records be kept of people who obtained prescriptions for certain addictive medications. Plaintiffs argued that the statute infringed upon their right to privacy. The Court held that the constitutionally protected “zone of privacy” extends to two distinct types of interests: (1) “independence in making certain kinds of important decisions”; and (2) the “individual interest in avoiding disclosure of personal matters.”⁴¹ The former interest referred to the line of cases beginning with *Griswold* which protected people’s right to make decisions about their health, bodies, and procreation. The latter interest, however, was one that the Court had not previously defined.

The plaintiffs argued that they feared the greater accessibility of their personal information and the potential for its disclosure. As a result of this fear, they argued, many patients did not get the prescriptions they needed and this interfered with their independence in making decisions with regard to their health. The Court, however, held that the constitutional right to information privacy required only a duty to avoid unreasonable disclosure, and that the state had taken adequate security measures.⁴²

The plaintiffs’ argument, however, was not that disclosure was the real privacy problem. Rather, the plaintiffs were concerned that the collection of and greater access to their information made them lose control over their information. A part of themselves—a very important part of their lives—was placed in the distant hands of the state and completely outside their control. This is similar to the notion of a chilling effect on free speech, which is not caused by the actual enforcement of a particular law but by the fear created by the very existence of the law. The Court acknowledged that the court record supported the plaintiffs’ contention that some people were so distraught over the law that they were not getting the drugs they needed. However, the Court rejected this argument by noting that because over 100,000 prescriptions had been filled before the law had been

enjoined, the public was not denied access to the drugs.⁴³ The problem with the Court's response is that the Court failed to indicate how many prescriptions had been filled before the law had been passed. Without this data, there is no way to measure the extent of the deterrence. And even if there were only a few who were deterred, the anxiety caused by living under such a regime must also be taken into account.

The famous case of *Doe v. Southeastern Pennsylvania Transportation Authority (SEPTA)* best illustrates how the constitutional right to information privacy fails to comprehend the privacy problem of databases.⁴⁴ The plaintiff Doe was HIV positive and told two doctors (Dr. Press and Dr. Van de Beek) at his work about his condition but nobody else. He strove to keep it a secret. His employer, SEPTA, a self-insured government agency, maintained a prescription drug program with Rite-Aid as the drug supplier. SEPTA monitored the costs of its program. Doe was taking a drug used exclusively in the treatment of HIV, and he asked Dr. Press whether the SEPTA officials who reviewed the records would see the names for the various prescriptions. Dr. Press said no, and Doe had his prescription filled under the plan. Unfortunately, even though SEPTA never asked for the names, Rite-Aid mistakenly supplied the names corresponding to prescriptions when it sent SEPTA the reports. Pierce, the SEPTA official reviewing the records, became interested in Doe's use of the drug and began to investigate. She asked Dr. Van de Beek about the drug, and he told her what the drug was used for but would not answer any questions about the person using the drugs. Pierce also asked questions of Dr. Press, who informed Doe of Pierce's inquiry.

This devastated Doe. Doe began to fear that other people at work had found out. He began to perceive that people were treating him differently. However, he was not fired, and in fact, he was given a promotion. The court of appeals held that the constitutional right to information privacy had not been violated because there had not been any disclosure of confidential information.⁴⁵ Pierce had merely informed doctors who knew already. Doe offered no proof that anybody else knew, and accordingly, the court weighed his privacy invasion as minimal.

However, this missed the crux of Doe's complaint. Regardless of whether he was imagining how his co-workers were treating him, he was indeed suffering a real, palpable fear. His injury was the powerlessness of having no idea who else knew he had HIV, what his employer thought of him, or how the information could be used against him. This feeling of unease changed the way he perceived everything at his place of employment. The privacy problem wasn't merely the fact that Pierce divulged his secret or that Doe himself had lost control over his information, but rather that the information appeared to be entirely out of anyone's control. Doe was in a situation similar to that of Kafka's Joseph K.—waiting endlessly for the final verdict. He was informed that information about him had been collected; he knew that his employer had been investigating; but the process seemed to be taking place out of his sight. To some extent, he experienced the desperation that Joseph K. experienced—he knew that information about him was out there in the hands of others and that these people were in fact doing something with that information, but he had no participation in the process.

Statutory Law

Since the early 1970s, Congress has passed over 20 laws pertaining to privacy. Unlike the European Union, which adopted a general directive providing for comprehensive privacy protection,⁴⁶ the United States has not enacted measures of similar scope. Instead, Congress has passed a series of statutes narrowly tailored to specific privacy problems.

The Fair Credit Reporting Act (FCRA) of 1970, which regulates credit reporting agencies, fails to adequately restrict secondary uses and disclosures of that information.⁴⁷ Although inspired by allegations of abuse and lack of responsiveness of credit agencies, the FCRA was severely weakened due to the effective lobbying of the credit reporting industry.⁴⁸ The Act permits credit reporting companies to sell the “credit header” portion of credit histories (which contains names, addresses, former addresses, telephone number, SSN, employment information, and birthdate) to marketers.⁴⁹ The FCRA does little to

equalize the unbalanced power relationship between individuals and credit reporting companies.

Congress's most significant piece of privacy legislation in the 1970s—the Privacy Act of 1974—regulates the collection and use of records by federal agencies, giving individuals the right to access and correct information in these records.⁵⁰ The Privacy Act is a good beginning, but it remains incomplete. In particular, it applies only to agencies of the federal government, and has no applicability to the use of databases by businesses and marketers.

The Family Educational Rights and Privacy Act of 1974 (FERPA), also known as the Buckley Amendment, regulates the accessibility of student records. The FERPA remains quite narrow, only applying to a subset of records in one limited context (education). Excluded are campus security records and health and psychological records.⁵¹

The Cable Communications Policy Act (CCPA) of 1984 requires cable operators to inform subscribers about the nature and uses of personal information collected.⁵² The law prohibits any disclosure that reveals the subscriber's viewing habits, and it is enforced with a private cause of action. The statute, however, applies only to cable operators and it has a broad exception where personal data can be disclosed for a "legitimate business activity." Nevertheless, the CCPA is an important first step in giving consumers control over their cable records.

In 1986, Congress modernized electronic surveillance laws when it passed the Electronic Communications Privacy Act (ECPA).⁵³ The ECPA extends the protections of the federal wiretap law of 1968 to new forms of voice, data, and video communications, including cellular phones and email. The ECPA restricts the interception of transmitted communications and the searching of stored communications. The focus of the law is on regulating surveillance. The difficulties of the ECPA in responding to the challenges of computer databases is illustrated by the case *In re DoubleClick, Inc. Privacy Litigation*.⁵⁴ A group of plaintiffs profled by DoubleClick contended that DoubleClick's placing and accessing cookies on their hard drives constituted unauthorized access in violation of ECPA. The court concluded that the ECPA didn't apply to DoubleClick because its cookies were perma-

ment and ECPA restricted unauthorized access only to communications in “temporary, intermediate storage.” Additionally, DoubleClick didn’t illegally intercept a communication in violation of the ECPA because DoubleClick was authorized to access the cookies by the websites that people visited. The *DoubleClick* case illustrates that the ECPA is not well-tailored to addressing a large portion of private-sector information gathering in cyberspace.

After reporters obtained Supreme Court Justice nominee Robert Bork’s videocassette rental data, Congress passed the Video Privacy Protection Act (VPPA) of 1988,⁵⁵ which has become known as the Bork Bill. The VPPA prohibits videotape service providers from disclosing the titles of the videos a person rents or buys. People are authorized to sue if the statute is violated.⁵⁶ However, the Act only applies to video stores, and no similar restrictions are placed on bookstores, record stores, or any other type of retailer, magazine producer, or catalog company.

The Telephone Consumer Protection Act (TCPA) of 1991 permits individuals to sue a telemarketer for damages up to \$500 for each call received after requesting not to be called again.⁵⁷ If the telemarketer knowingly breaks the law, then the penalty is trebled. The TCPA, however, aims at redressing the aggravation of disruptive phone calls, and it does not govern the collection, use, or sale of personal data.

In 1994, Congress finally addressed the longstanding practice of many states of selling personal information in their motor vehicle records to marketers. The Driver’s Privacy Protection Act of 1994 (DPPA) limits this practice, forcing states to acquire a driver’s consent before disclosing personal information to marketers.⁵⁸ Although the DPPA is an important step in controlling government disclosures of personal information to the private sector, it applies only in the context of motor vehicle records. States are not limited in disclosing information contained in the numerous other forms of records they maintain.

In 1996, Congress passed the Health Insurance Portability and Accountability Act (HIPAA) to help standardize medical information so it could be transferred more easily between different databases.⁵⁹ Since this raised privacy concerns, Congress ordered the Department

of Health and Human Services (HHS) to regulate the privacy of medical records. HHS's regulations, among other things, require authorization for all uses and disclosures beyond those for treatment, payment, or health care operation (such as for marketing purposes).⁶⁰ The HIPAA regulations have apparently pleased nobody. Doctors and hospitals complain that the regulations are too complicated, cumbersome, and expensive to follow. Advocates for privacy find the regulations weak and ineffective.

The first federal law directly addressing privacy in cyberspace, the Children's Online Privacy Protection Act (COPPA) of 1998, regulates the collection of children's personal information on the Internet.⁶¹ Websites targeted at children must post privacy policies and must obtain parental consent in order to use children's personal information. But the law's reach is limited. It applies only to children's websites or when the website operator "has actual knowledge that it is collecting personal information from a child."⁶² Only children under age 13 are covered. Additionally, as privacy law expert Anita Allen argues, the law forces parents to become involved in their children's Internet activities when some parents "may want their children to have free access to the Internet for moral or political reasons." Allen concludes that "COPPA is among the most paternalistic and authoritarian of the federal privacy statutes thus far."⁶³

The Gramm-Leach-Bliley (GLB) Act of 1999 permits any financial institution to share "nonpublic personal information" with affiliated companies.⁶⁴ However, people can opt-out when a company discloses personal information to third parties.⁶⁵ In practice, the GLB Act greatly facilitates the disclosure of people's information. Given the large conglomerates of today's corporate world, affiliate sharing is significant. For example, Experian, one of the three largest credit reporting agencies, was purchased by Great Universal Stores, a British retail corporation, which also acquired Metromail, Inc., a direct-marketing company.⁶⁶ The Act applies only to "nonpublic" information, and much of the information aggregated in databases (such as one's name, address, and the like) is often considered to be public. Additionally, the Act's opt-out right is ineffective. As legal scholars Ted Janger and Paul Schwartz argue, the financial institution has "superior knowledge" and the GLB "leaves the burden of bargaining on the

less informed party, the individual consumer.”⁶⁷ They conclude that “[a]n opt-out default creates incentives for privacy notices that lead to *inaction* by the consumer.”⁶⁸

In sum, the federal laws are a start, but they often give people only a very limited form of control over only some of their information and frequently impose no system of default control on other holders of such information.⁶⁹ Although the statutes help in containing the spread of information, they often fail to adequately address the underlying power relationships and contain broad exceptions and loopholes that limit their effectiveness.

Furthermore, the federal statutes cover only a small geography of the database problem. As privacy law expert Joel Reidenberg has pointed out, the laws are “sectoral” in nature, dealing with privacy in certain contexts but leaving gaping holes in others.⁷⁰ “This mosaic approach,” he observes, “derives from the traditional American fear of government intervention in private activities and the reluctance to broadly regulate industry. The result of the mosaic is a rather haphazard and unsatisfactory response to each of the privacy concerns.”⁷¹

Thus, the federal privacy statutes form a complicated patchwork of regulation with significant gaps and omissions. For example, federal regulation covers federal agency records, educational records, cable television records, video rental records, and state motor vehicle records, but it does not cover most records maintained by state and local officials, as well as a host of other records held by libraries, charities, and merchants (i.e., supermarkets, department stores, mail order catalogs, bookstores, and the like). The COPPA protects the privacy of children under 13 on the Internet, but there is no protection for adults. As political scientist Colin Bennett observes, “[t]he approach to making privacy policy in the United States is reactive rather than anticipatory, incremental rather than comprehensive, and fragmented rather than coherent. There may be a lot of laws, but there is not much protection.”⁷²

Second, many of Congress’s privacy statutes are hard to enforce. It is often difficult, if not impossible, for an individual to find out if information has been disclosed. A person who begins receiving unsolicited marketing mail and email may have a clue that some entity has disclosed her personal information, but that person often will not be

able to discover which entity was the culprit. Indeed, the trade in personal information is a clandestine underworld, one that is not exposed sufficiently by federal privacy regulation to enable effective enforcement.

The Kafka metaphor illustrates that the problem with digital dossiers involves the fact that our personal information is not only out of our control but also is often placed within a bureaucratic process that lacks control and discipline in handling and using such information. The federal statutes have certainly made advances in protecting against this problem, and they demonstrate that Congress's resolve to protect privacy has remained strong for over 30 years. But much more work remains to be done.

The FTC and Unfair and Deceptive Practices

Since 1998, the Federal Trade Commission (FTC) has been bringing actions against companies that violate their own privacy policies. The FTC has interpreted the FTC Act, which prohibits "unfair or deceptive acts or practices in or affecting commerce,"⁷³ to be infringed when a company breaks a promise it made in its privacy policy. The FTC can bring civil actions and seek injunctive remedies. Since it began enforcing the Act in this manner, the FTC has brought several high-profile cases, almost all of which have resulted in settlements.⁷⁴

Yet, the FTC has been rather weak and reactive in its enforcement of privacy policies.⁷⁵ In a number of cases involving companies engaging in blatant breaches of their own privacy policies, the FTC has settled, simply requiring companies to sin no more.⁷⁶ A recent case involving Microsoft, however, suggests that the FTC might become more proactive. Microsoft's Passport maintains the personal information of Internet users to allow them to use a single username and password to access many different websites without having to sign on to each separately. Although Microsoft promised in its privacy policy that it protected Passport information with "powerful online security technology," the FTC concluded that Microsoft did not provide adequate security. Microsoft and the FTC agreed on a settlement where Microsoft must create a better system of security.⁷⁷ Unlike most cases

before the FTC, the security problems of Microsoft's Passport had not yet resulted in a major security breach.

In the end, however, the FTC is limited in its reach. It only ensures that companies keep their promises. As Paul Schwartz notes, if a website doesn't make a promise about privacy, then it will "fall outside of the FTC's jurisdiction."⁷⁸ Unfortunately, the FTC has only limited time and resources, and its "privacy protection activities already are dwarfed by its more aggressive investigations of fraud and deceptive marketing practices on the Internet."⁷⁹

A World of Radical Transparency: Freedom of Information Law

Some commentators suggest that there is little the law can do to protect privacy in the Information Age. In *The Transparent Society*, technology commentator David Brin argues that privacy is dead:

[I]t is already far too late to prevent the invasion of cameras and databases. The *djinn* cannot be crammed back into its bottle. No matter how many laws are passed, it will prove quite impossible to legislate away the new surveillance tools and databases. They are here to stay. Light *is* going to shine into every corner of our lives.⁸⁰

Brin suggests that we abandon privacy in favor of a transparent society, one where everything is out in the open, where we watch the watchers, where we have the ability to monitor the elites—the politicians and the corporate leaders—just as much as they have the ability to monitor us. "[W]e may not be able to eliminate the intrusive glare shining on citizens of the [twenty-first century]," Brin observes, "but the glare just might be rendered harmless through the application of more light aimed in the other direction."⁸¹ We should thus regulate in favor of mandating free access to information. According to Brin, a truly transparent society would hold accountable those who would violate our privacy.⁸²

Brin fails to realize that affording mutuality of access to information will do little to empower ordinary individuals. The reason is that information is much more of an effective tool in the hands of a large

bureaucracy. Information is not the key to power in the Information Age—knowledge is. Information consists of raw facts. Knowledge is information that has been sifted, sorted, and analyzed. The mere possession of information does not give one power; it is the ability to process that information and the capability to use the data that matter. In order to solve the problem, a transparent society would have to make each individual as competent as bureaucratic organizations in processing information into knowledge.

The Law of Information Privacy and Its Shortcomings

As this chapter has demonstrated, the law of information privacy is quite extensive. It developed in response to certain vexing privacy problems, often created by new technologies. The Warren and Brandeis privacy torts were inspired by new photographic technology and a rapidly growing media that was becoming very sensationalistic. The types of injuries Warren and Brandeis had in mind were those caused by intrusive newsgathering techniques and by publishing private information in the newspapers. In the mid-twentieth century, during the Cold War, the law focused heavily on surveillance, which had become one of the central threats to privacy. These times witnessed the growth of electronic communication along with new means of electronic espionage such as wiretapping, bugging devices, and video cameras. Americans feared the terrible totalitarian regimes of Nazi Germany, the Soviet Union, and Eastern Europe, all of which employed extensive monitoring of their citizens' private lives as well as secret police and spies to maintain strict control. Law enforcement officials in the United States also increasingly resorted to the use of surveillance, with the rapidly growing FBI leading the way. It is therefore certainly not surprising that the privacy law forged during these times was devoted to ameliorating the kinds of harms so perfectly captured in Orwell's *1984*.

However, the advent of the computer, the proliferation of databases, and the birth of the Internet have created a new breed of privacy problems. The Orwellian dangers have certainly not disappeared; nor have the harms created by the sensationalistic media. But the rise of digital dossiers has created new and different

problems. New privacy laws have been created in response. The constitutional right to information privacy has emerged in the courts as a spinoff of the regular constitutional right to privacy. Congress and the states have passed numerous statutes to regulate the collection and use of personal information. The FTC has started to bring enforcement actions against companies that fail to live up to their privacy promises. All of these developments have been promising, but as I have shown throughout this chapter, the law of privacy has not dealt effectively with the new problems created by digital dossiers. The reason is that the law still harbors conceptions of privacy that are not responsive to the realities of the Information Age. These new privacy problems are not isolated infringements, but are systematic and diffuse. They are often not created by a single perpetrator, but by a combination of actors often without sinister purposes. The problems caused by digital dossiers are quite broad, and they apply to the entire information economy, making the narrow federal statutes inapplicable to a large portion of the flow of personal information. Enforcing rights and remedies against the collection and use of personal information is very difficult since much information flow occurs without people even knowing about it.

So what can be done? I have demonstrated some of the law's shortcomings. Can the law adequately respond to these problems? This question will be the focus of the next chapter and beyond.