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
In loving memory of

my grandma,

Jean
Contents

Acknowledgments ix

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

2 The Rise of the Digital Dossier 13
   A History of Public-Sector Databases 13
   A History of Private-Sector Databases 16
   Cyberspace and Personal Information 22

3 Kafka and Orwell: 27
   Reconceptualizing Information Privacy 27
   The Importance of Metaphor 27
   George Orwell's Big Brother 29
The Impact of Technology 131
The Regulation of Public Records 132

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

iii government access

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

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

11 Reconstructing the Architecture 210
  Scope: System of Records 211
  Structure: Mechanisms of Oversight 217
  Regulating Post-Collection Use of Data 221
  Developing an Architecture 222
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.
The problems arising from the emergence of digital dossiers are profoundly important. They affect the power of individuals, institutions, and the government; and they pervade numerous relationships that form the framework of modern society. The way we respond to these problems will significantly shape the type of society we are constructing. Digital dossiers will affect our freedom and power; they will define the very texture and tenor of our lives.

Ideally, technology empowers us, gives us greater control over our lives, and makes us more secure. But digital technologies of data gathering and use are having the opposite effect. Increasingly, companies and the government are using computers to make important decisions about us based on our dossiers, and we are frequently not able to participate in the process.

As discussed throughout this book, the law of information privacy has not yet effectively grappled with these problems. Certainly, information privacy law has had positive effects. It would be far too simple to conclude that the law has failed. But the law has not been sufficiently successful, and the problems have grown much more troubling during the law’s watch.
One response to these developments is a cynical one. Some commentators argue that things have already progressed too far for law to grapple with the problems of digital dossiers. Scott McNealy, CEO of Sun Microsystems, famously quips: “You already have zero privacy. Get over it.” Amitai Etzioni observes that “as long as Americans wish to enjoy the convenience of using credit cards and checks (as opposed to paying cash) and of ordering merchandise over the phone and the Internet (rather than shopping in person), they will leave data trails that are difficult to erase or conceal.” “To be realistic,” Etzioni states, “the probability of returning the genie to the bottle is nil.”

Too often, discussions of privacy parade a horde of horribles, raising fears of new technologies developing too fast for the law to handle. We are left with a sense of hopelessness—technology will continue to erode privacy and there is little we can do to stop it. To the contrary, I believe that there is much cause for optimism. We are still in the early days of the Information Age, and we still have the ability to shape the networks of information flow.

In fact, technology isn’t the primary culprit—many of the privacy problems I discussed are caused in large part because of the law. The law plays a profound role not just in solving the problems of digital dossiers, but in manufacturing them as well. The law is not merely reactive to new technologies that threaten privacy, but is also a shaping force behind these technologies as well as the amount of privacy we experience today. We often see privacy as naturally occurring and threatened by rapidly developing technology. Law must intervene to protect privacy. However, law creates and constructs the world we live in. This is particularly true with privacy. To a significant degree, privacy is legally constructed. Law already shapes our ability to hide information and it shapes information accessibility. Law makes certain information publicly available; it keeps places (such as the home) private by enforcing trespass and property laws. Law also shapes our expectations of privacy in many contexts.

The law also influences much of the loss of privacy. Many privacy problems are the product of legal decisions that have been made over the past century as we have shaped our modern information economy. Once we understand the full extent of the legal construction of
privacy, we will realize that privacy is not passively slipping away but is being actively eliminated by the way we are constructing the information economy through the law.

In the nineteenth century, Americans faced many significant privacy problems. For example, since colonial times, the privacy of the mail was a vexing problem. Sealing letters was difficult.\(^5\) Benjamin Franklin, who was in charge of the colonial mails, required his employees to swear an oath not to open mail.\(^6\) Nevertheless, significant concerns persisted about postal clerks reading people's letters. Thomas Jefferson, Alexander Hamilton, and George Washington frequently complained about the lack of privacy in their letters, and they would sometimes write in code.\(^7\) As Thomas Jefferson wrote: “[T]he infidelities of the post office and the circumstances of the times are against my writing fully and freely.”\(^8\)

These problems persisted in the nineteenth century. As Ralph Waldo Emerson declared, it was unlikely that “a bit of paper, containing our most secret thoughts, and protected only by a seal, should travel safely from one end of the world to the other, without anyone whose hands it had passed through having meddled with it.”\(^9\) The law responded to these problems. Congress passed several strict laws protecting the privacy of the mail.\(^10\) And in 1877, in *Ex Parte Jackson*, the Supreme Court held that the Fourth Amendment prohibited government officials from opening letters without a warrant.\(^11\)

In the nineteenth century, one might have simply concluded that people shouldn't expect privacy in their letters, and that they should “get over it.” But privacy isn't just found but constructed. It is the product of a vision for a future society. By erecting a legal structure to protect the privacy of letters, our society shaped the practices of letter-writing and using the postal system. It occurred because of the desire to make privacy an integral part of these practices rather than to preserve the status quo.

Similar examples abound in the nineteenth and early twentieth centuries. When the increasing amount of information collected by the U.S. census sparked a public outcry, Congress took action by passing powerful laws to safeguard the confidentiality of census information.\(^12\) After Warren and Brandeis's 1890 article, *The Right to Privacy*,\(^13\) raised concern over new technologies in photography and an
increasingly sensationalistic press, courts and legislatures responded by creating many new privacy laws.

Today, we face new technological challenges. Many of the problems we currently encounter are created by the profound growth in the creation and use of digital dossiers. Part of the difficulty we are experiencing in dealing with these problems is that they are not as easy to capture in a soundbite, and they often do not quickly materialize as concrete injuries. When a scandalous secret is disclosed or a hidden video camera is installed in one's bedroom, we can easily recognize and describe the privacy harms. The troubles caused by digital dossiers are of a different sort. These harms are complex and abstract, which is why I invoked the metaphor of Kafka's *The Trial*, since Kafka was so adept at depicting these types of harms. Today, like the all-encompassing Court system that assembled a dossier about Joseph K., large organizations we know little about are producing digital dossiers about us. The dossiers capture a kind of digital person—a personality translated into digitized form, composed of records, data fragments, and bits of information. Our digital dossiers remain woefully insecure, at risk of being polluted by identity thieves or riddled with careless errors. And all the while, we are like Joseph K.—powerless, uncertain, and uneasy—constantly kept on the outside while important decisions about us are being made based on our dossiers.

I have argued that we need to rethink traditional notions of privacy in order to solve these problems. Protecting privacy in the Information Age is a question of social design. It is about designing an architecture for the information networks that are increasingly constitutive of modern society. The law must restructure our relationships with the entities collecting and using our personal information. These relationships are not naturally occurring—it is the law that has defined our relationships to various businesses and institutions, and it is thus the law that is at least partly responsible for our powerlessness and vulnerability. Changing our relationships with bureaucracies can't be achieved through isolated lawsuits. We need a regulatory system, akin to the ones we have in place regulating our food, environment, and financial institutions.
The law actively contributes to the creation of our dossiers by compelling people to give up personal data, placing it in public records, and then allowing it to be amassed by database companies. The solution is for the law to place greater controls on its public records by limiting the degree to which personal information in these records can be accessed and used.

The increasing government access and use of our digital dossiers is also the product of legal decisions made during the past century. The Supreme Court has interpreted the Fourth Amendment in a shortsighted way, and the use of dossiers threatens a profound end-run around Fourth Amendment protections. The law that fills the void fails to adequately control the government’s tapping into our digital dossiers. The solution is to create a legal structure for keeping government access to our digital dossiers in check. The government should be required to obtain a special court order when it wants to access personal data that is maintained in a business’s record systems.

All of these solutions are not absolutist ones. I am not advocating that businesses be forbidden from collecting personal data or that public records be made inaccessible or that the government be prohibited from obtaining personal information. These absolutist solutions are not practical in an information society. In this respect, those that say the genie can’t be stuffed back into the bottle are correct. We will not suddenly turn into Luddites and throw away our credit cards, stop surfing the Internet, and return to using paper records. We are in an Information Age, and there is no turning back. But this does not mean that privacy is destined for extinction. We can have the benefits of an information-driven world without sacrificing privacy. The solutions I propose do not stop the flow of data. Companies can still gather information; public records can be made widely available; and the government can obtain personal information. But when companies collect our data, the law should impose weighty responsibilities and should allow people to have greater participation in how the data is used. When public records are made available, the law should do so along with demanding restrictions on access and use. When the government wants to obtain personal data, the law should mandate that it demonstrate before a neutral judicial official that it has a factual
basis that the search will reveal evidence of a particular person’s criminal activity.

The law can protect privacy. This does not require that the law become involved in areas in which it currently has been absent—the law is already involved. The choices we make in shaping the law are of critical importance. The law is currently making choices, and it is attempting to balance privacy against countervailing interests such as efficiency, transparency, free speech, and safety. As I have demonstrated throughout this book, however, our understandings of privacy must be significantly rethought. Once privacy is reconceptualized, we can find ways to accommodate both privacy and its opposing interests. With an understanding of privacy appropriate for the problems we now face, the law will be better able to build privacy into our burgeoning information society.