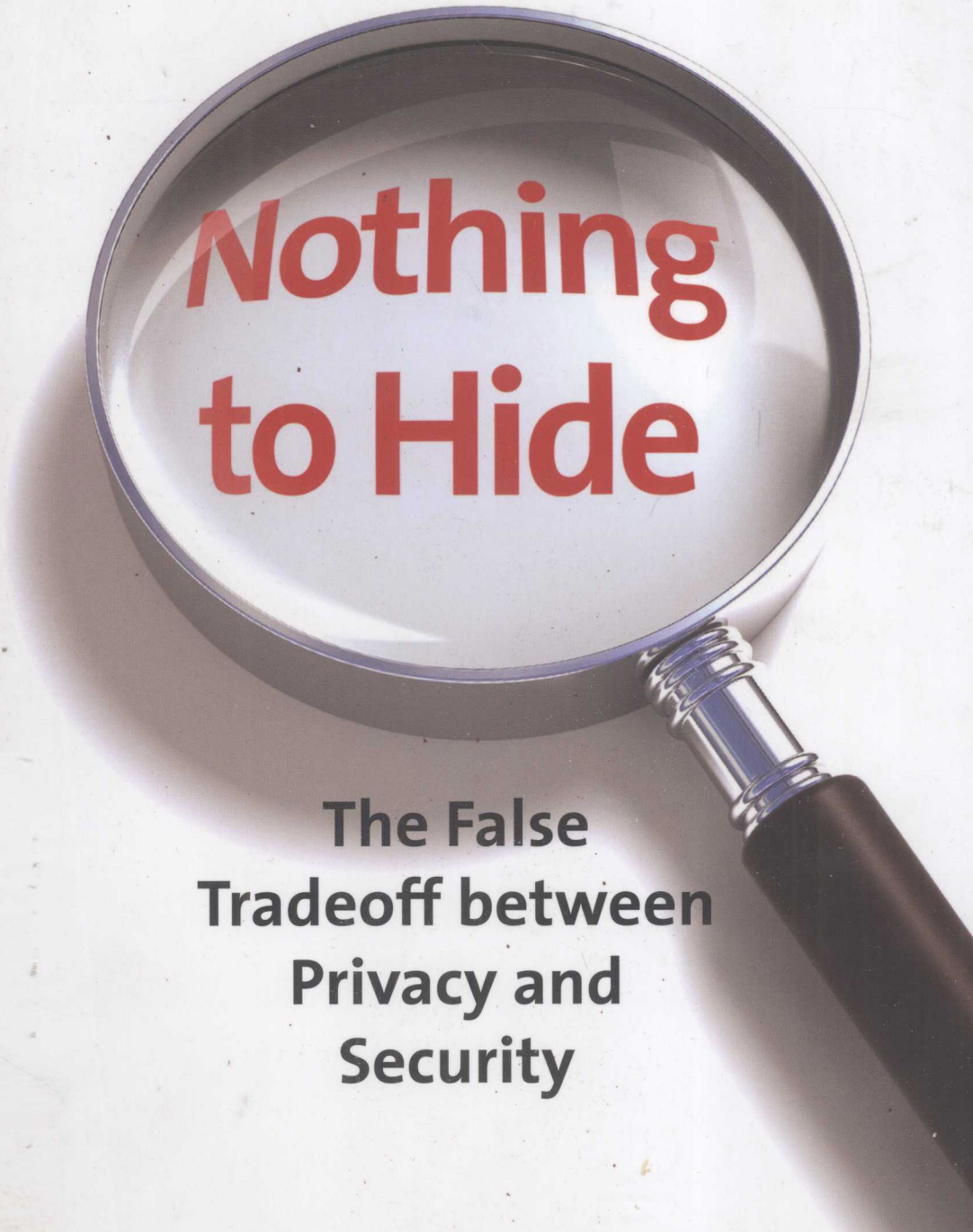
DANIEL J. SOLOVE



Nothing to Hide

The False Tradeoff between Privacy and Security

To Pamela and Griffin, with love

Set in Electra type by Integrated Publishing Solutions.
Printed in the United States of America.

Library of Congress Cataloging-in-Publication Data

Solove, Daniel J., 1972–
Nothing to hide : the false tradeoff between privacy and security / Daniel J. Solove.
p. cm.
Includes bibliographical references and index.
ISBN 978-0-300-17231-7 (cloth : alk. paper) 1. Privacy, Right of—United States. 2. Law enforcement—United States 3. National security—Law and legislation—United States I. Title.
KF1262.S65 2011
342.7308'58—dc22 2010049542

A catalogue record for this book is available from the British Library.

This paper meets the requirements of ANSI/NISO Z39.48–1992 (Permanence of Paper).

10 9 8 7 6 5 4 3 2 1

Nothing to Hide

Preface

The idea for this book began with an essay I wrote a few years ago called *"I've Got Nothing to Hide" and Other Misunderstandings of Privacy*. After I posted it online, I was stunned by the attention it received across the Internet and in the media. I realized that there was a lot of interest in the debate between privacy and national security and that the same group of arguments came up again and again. I also realized that there were many misimpressions about the law.

Increasingly, I've found it frustrating when I hear certain arguments in favor of heightened security that have become quite prevalent. I believe they have skewed the balance between privacy and security too much to the security side. One of my goals in this book is to respond to some of these arguments.

I have written this book for a general audience, avoiding legal jargon and wonky policy analysis. I've presented more detailed policy proposals in my law review articles, but for this book, I focus on the general arguments and principles rather than technical minutiae. Of course, the details are important, but even more important are the basic concepts and themes of the debate. I hope that this book will put to rest certain arguments so that the debate can move ahead in more fruitful ways.

Although I have focused primarily on American law, the ar-

guments and ideas in the debate are universal. Despite a few differences, the law in many countries operates similarly to American law, and it often uses the same techniques to regulate government information gathering. The arguments and policy recommendations I propose in this book are meant to be relevant not just in the United States but also in other nations whose lawmakers are struggling with these important issues.

Some of the material for this book was adapted from a few of my law review articles. These articles are much more extensive than their adaptations in this book, and they are often very different in form and argument. I have not fully incorporated these articles here, so they remain independent works. I recommend that you check them out if you want a more technical treatment of some of the issues in this book: *Fourth Amendment Pragmatism*, 51 BOSTON COLLEGE LAW REVIEW (forthcoming); *Data Mining and the Security-Liberty Debate*, 74 UNIVERSITY OF CHICAGO LAW REVIEW 343 (2008); *"I've Got Nothing to Hide" and Other Misunderstandings of Privacy*, 44 SAN DIEGO LAW REVIEW 745 (2007); *The First Amendment as Criminal Procedure*, 84 NEW YORK UNIVERSITY LAW REVIEW 112 (2007); *Fourth Amendment Codification and Professor Kerr's Misguided Call for Judicial Deference*, 74 FORDHAM LAW REVIEW 747 (2005); *Melville's Billy Budd and Security in Times of Crisis*, 26 CARDOZO LAW REVIEW 2443 (2005); *Reconstructing Electronic Surveillance Law*, 72 GEORGE WASHINGTON LAW REVIEW 1264 (2004). My thinking has evolved since the publication of many of these articles, so this book represents my most current view of the issues. Moreover, writing this book forced me to think more broadly about the topic of privacy versus security, and there are many issues I address here that I haven't addressed before.

Many people helped me greatly with this project. My wife, Pamela, provided constant support and encouragement as well as superb suggestions on the manuscript. Many others have made immensely helpful comments on this book: Danielle Citron, Tommy

Crocker, Deven Desai, Chris Hoofnagle, Orin Kerr, Raymond Ku, Paul Ohm, Neil Richards, and Michael Sullivan. I would also like to thank my research assistant, Matthew Albanese, for his help. My editor, Michael O'Malley, was a joy to work with, and my copyeditor, Dan Heaton, carefully reviewed the manuscript. My agent, Susan Schulman, provided excellent guidance and encouragement throughout the publication process.

Contents

1

Introduction

"We must be willing to give up some privacy if it makes us more secure."

"If you've got nothing to hide, you shouldn't worry about government surveillance."

"We shouldn't second-guess security officials."

"In national emergencies, rights must be cut back, but they'll be restored later on."

We hear these arguments all the time. We hear them in the conversations we have each day with our family, friends, and colleagues. We hear them in the media, which is buzzing with stories about government information gathering, such as the Total Information Awareness program, the airline passenger screening program, and the surveillance of people's phone calls conducted by the secretive National Security Agency. We hear them made by politicians and security officials. And we hear them made by judges deciding how to balance security measures with people's constitutional rights.

These arguments are part of the debate between privacy and security. The consequences of the debate are enormous, for both privacy and security are essential interests, and the balance we strike between them affects the very foundations of our freedom and democracy. In contemporary times—especially after the terrorist attacks on September 11, 2001—the balance has shifted toward the security

side of the scale. The government has been gathering more information about people and engaging in more surveillance. Technology is giving the government unprecedented tools for watching people and amassing information about them—video surveillance, location tracking, data mining, wiretapping, bugging, thermal sensors, spy satellites, X-ray devices, and more. It's nearly impossible to live today without generating thousands of records about what we watch, read, buy, and do—and the government has easy access to them.

The privacy-security debate profoundly influences how these government activities are regulated. But there's a major problem with the debate: Privacy often loses out to security when it shouldn't. Security interests are readily understood, for life and limb are at stake, while privacy rights remain more abstract and vague. Many people believe they must trade privacy in order to be more secure. And those on the security side of the debate are making powerful arguments to encourage people to accept this tradeoff.

These arguments, however, are based on mistaken views about what it means to protect privacy and the costs and benefits of doing so. The debate between privacy and security has been framed incorrectly, with the tradeoff between these values understood as an all-or-nothing proposition. But protecting privacy need not be fatal to security measures; it merely demands oversight and regulation. We can't progress in the debate between privacy and security because the debate itself is flawed.

The law suffers from related problems. It seeks to balance privacy and security, but systematic problems plague the way the balancing takes place. When evaluating security measures, judges are often too deferential to security officials. And the law gets caught up in cumbersome tests to determine whether government information gathering should be subjected to oversight and regulation, resulting in uneven and incoherent protection. The law sometimes stringently protects against minor privacy invasions yet utterly fails to protect

against major ones. For example, the Fourth Amendment will protect you when a police officer squeezes the outside of your duffel bag—yet it won't stop the government from obtaining all your Google search queries or your credit card records.

The privacy-security debate and the law have a two-way relationship. Many arguments in the debate are based on false assumptions about how the law protects privacy. And the law has been shaped by many flawed arguments in the debate, which have influenced legislation and judicial opinions.

I propose to demonstrate how privacy interests can be better understood and how security interests can be more meaningfully evaluated. I aim to refute the recurrent arguments that skew the privacy-security debate toward the security side. I endeavor to show how the law frequently fixes on the wrong questions, such as *whether* privacy should be protected rather than *how* it should be protected. Privacy often can be protected without undue cost to security. In instances when adequate compromises can't be achieved, the tradeoff can be made in a manner that is fair to both sides. We can reach a better balance between privacy and security. We must. There is too much at stake to fail.

A Short History of Privacy and Security

The law and policy addressing privacy and security is quite extensive, involving the U.S. Constitution, federal statutes, state constitutions, and state statutes. Quite a number of federal agencies are involved, such as the Federal Bureau of Investigation (FBI), Central Intelligence Agency (CIA), National Security Agency (NSA), Department of Homeland Security (DHS), Transportation Security Administration (TSA), and others. There are countless state and local police departments. In order to understand how privacy and security are balanced, I will first explain briefly how we got to where we are today.

The Right to Privacy

People have cared about privacy since antiquity. The Code of Hammurabi protected the home against intrusion, as did ancient Roman law.[1] The early Hebrews had laws safeguarding against surveillance. And in England, the oft-declared principle that the home is one's "castle" dates to the late fifteenth century.[2] Eavesdropping was long protected against in the English common law, and in 1769, the legal scholar William Blackstone defined it as listening "under walls or windows, or the eaves of a house, to hearken after discourse, and thereupon to frame slanderous and mischievous tales."[3]

The right to privacy emerged in countries all around the world in many different dimensions. Protections arose against invasions of privacy by nosy neighbors and gossipy newspapers, as well as against government searches and seizures. In England, for example, the idea that citizens should be free from certain kinds of intrusive government searches developed during the early 1500s.[4]

In America, at the time of the Revolutionary War, a central privacy issue was freedom from government intrusion. The Founders detested the use of general warrants to conduct sweeping searches of people's homes and to seize their papers and writings.[5] As Patrick Henry declared: "They may, unless the general government be restrained by a bill of rights, or some similar restrictions, go into your cellars and rooms, and search, ransack, and measure, everything you eat, drink, and wear. They ought to be restrained within proper bounds."[6]

These sentiments were enshrined into the Bill of Rights. The Fourth Amendment to the U.S. Constitution prevents the government from conducting "unreasonable searches and seizures." Government officials must obtain judicial approval before conducting a search through a warrant that is supported by probable cause. The Fifth Amendment affords individuals a privilege against being compelled to incriminate themselves.

The Rise of Police Systems and the FBI

Security is also a universal value, tracing back to antiquity. People have long looked to their governments to keep them secure from bandits, looters, and foreign invaders. They have also wanted to ensure social order by protecting against robberies, rapes, murders, and other crimes. But for a long time, many countries lacked police forces. In medieval England, for example, posses hunted down criminals and summarily executed them. Later on, patrolling amateurs protected communities, but they rarely investigated crimes.[7]

By the twentieth century, police forces had transformed into organized units of professionals.[8] In the United States, policing developed locally at the city and state levels, not nationwide. The rise of the mafia and organized crime required law enforcement to find means to learn about what crimes these groups were planning. The government began to increase prosecution of certain consensual crimes, such as gambling, the use of alcohol during Prohibition, and the trafficking of drugs. Unlike robberies or assaults, which are often reported to the police, these crimes occurred through transactions in an underground market. Undercover agents and surveillance became key tools for detecting these crimes.

The FBI emerged in the early years of the twentieth century, the brainchild of Attorney General Charles Bonaparte. He twice asked Congress to authorize the creation of a detective force in the Department of Justice (DOJ), but he was rebuffed both times.[9] Congress worried about secret police prying into the privacy of citizens. As one congressman declared, "In my reading of history I recall no instance where a government perished because of the absence of a secret-service force, but many there are that perished as a result of the spy system."[10]

But Bonaparte was not deterred. He formed a new subdivision of the DOJ called the Bureau of Investigation, and brought in people from other agencies to staff it. In 1908 President Theodore Roosevelt issued an executive order authorizing the subdivision.

Table 1 Growth of the FBI

Year	Agents	Support Staff
1933	353	422
1945	4,380	7,422
2008	12,705	17,871

J. Edgar Hoover soon took the helm of the Bureau, which was renamed the FBI in 1935.[11]

Throughout the rest of the century, the FBI grew dramatically (see Table 1). During President Franklin Roosevelt's tenure, the size of the FBI increased more than 1000 percent.[12] It has continued to grow, tripling in size over the past sixty years.[13] Despite its vast size, extensive and expanding responsibilities, and profound technological capabilities, the FBI still lacks the congressional authorizing statute that most other federal agencies have.

The Growth of Electronic Surveillance

The FBI came into being as the debate over surveillance of communications entered a new era. Telephone wiretapping technology appeared soon after the invention of the telephone in 1876, making the privacy of phone communications a public concern. State legislatures responded by passing laws criminalizing wiretapping.

In 1928, in *Olmstead v. United States,* the U.S. Supreme Court held that the Fourth Amendment did not apply to wiretapping. "There was no searching," the Supreme Court reasoned. "There was no seizure. The evidence was secured by the use of the sense of hearing and that only. There was no entry of the houses or offices of the defendants."[14] Justice Louis Brandeis penned a powerful dissent, arguing that new technologies required rethinking old-fashioned notions of the Fourth Amendment: "Subtler and more far-reaching

means of invading privacy have become available to the government. Discovery and invention have made it possible for the government, by means far more effective than stretching upon the rack, to obtain disclosure in court of what is whispered in the closet." He also mentioned that the Founders of the Constitution "conferred, as against the government, the right to be let alone—the most comprehensive of rights and the right most valued by civilized men. To protect that right, every unjustifiable intrusion by the government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment."[15]

In 1934, six years after *Olmstead*, Congress passed a law to prohibit wiretapping.[16] But the law was largely ineffective, since it was interpreted only to preclude the introduction of wiretapping evidence in court.[17] The government could wiretap freely so long as it did not seek to use the product as evidence at trial.

During World War II and the ensuing Cold War, presidents gave the FBI new authorization to engage in wiretapping.[18] J. Edgar Hoover, still at the helm of the FBI, ordered wiretapping of hundreds of people, including dissidents, Supreme Court justices, professors, celebrities, writers, and others. Among Hoover's files were dossiers on John Steinbeck, Ernest Hemingway, Charlie Chaplin, Marlon Brando, Muhammad Ali, Albert Einstein, and numerous presidents and members of Congress.[19] When Justice William Douglas complained for years that the Supreme Court was being bugged and tapped, he seemed paranoid—but he was right.[20]

Protecting National Security: New Agencies and More Surveillance

During the 1940s and 1950s, enormous threats to national security loomed on the horizon. Concerns about the spread of communism and the Cold War with the Soviet Union led to an increased need for the government to engage in spying and foreign intelligence

gathering. In 1942 President Roosevelt created the Office of Strategic Services (OSS) to engage in these activities, but it was eliminated after World War II. Just a few years later, however, President Truman revived the OSS's activities by creating the modern CIA with the National Security Act of 1947.

In 1952 Truman created the National Security Agency (NSA) to handle cryptology—the breaking of encryption codes so that any foreign communications collected could be analyzed. For a long time, the NSA operated with a low profile, and the few in the know quipped that its acronym stood for "No Such Agency."

Domestically, fears grew that communism was a threat not just from abroad but also from within. In the 1950s the FBI began the Counter Intelligence Program (COINTELPRO) to gather information about political groups viewed as national security threats. The FBI's tactics included secretly attempting to persuade employers to fire targeted individuals, anonymously informing spouses of affairs to break up marriages, and using the threat of Internal Revenue Service investigations to deter individuals from attending meetings and events.[21] The primary target was the American Communist Party, but by the late 1950s and early 1960s, COINTELPRO had expanded its interests to include members of the civil rights movement and opponents of the Vietnam War.[22] Included among these individuals was Martin Luther King, Jr., whom Hoover had under extensive surveillance. FBI recordings revealed that King was having extramarital affairs, and the FBI sent copies of the recordings to King and his wife, threatening that if King failed to commit suicide by a certain date, the recordings would be released publicly.[23]

The Criminal Procedure Revolution

In the 1960s the U.S. Supreme Court, led by Chief Justice Earl Warren, radically transformed criminal procedure. Police sys-

tems around the country had grown substantially, and the FBI and other federal law-enforcement agencies were increasingly active. There wasn't much law regulating how the government could go about collecting information about people.

To fill this void, the Supreme Court began boldly interpreting the Fourth and Fifth Amendments to regulate what law-enforcement officials could search and seize as well as how they could question suspects. In 1961, in *Mapp v. Ohio*, the Supreme Court held that evidence obtained in violation of the Fourth Amendment must be excluded from evidence in criminal trials.[24] In 1967 the Supreme Court overruled *Olmstead* in *United States v. Katz*, declaring that wiretapping was covered by the Fourth Amendment.[25] The Court articulated a broad test for the scope of Fourth Amendment protection—it would apply whenever the government violated a person's "reasonable expectation of privacy." In 1968, just a year after *Katz*, Congress enacted a law to better regulate electronic surveillance.[26] The law provided strict controls on government wiretapping and bugging.

Thus, through the efforts of the Supreme Court and Congress, legal regulation of government information gathering expanded significantly in the 1960s.

Regulating National Security Surveillance

An open question, however, existed for matters of national security. Were they to be treated differently from regular criminal investigations? In 1972 the U.S. Supreme Court addressed the question but didn't provide a definitive answer. It concluded that the Fourth Amendment applied to government surveillance for national security, though the rules to regulate it might differ from those involving ordinary crime.[27]

J. Edgar Hoover died in 1972, while still head of the FBI. He had been its director for nearly fifty years. Many presidents and mem-