Nothing to Hide

The False Tradeoff between Privacy and Security

Daniel J. Solove

Yale UNIVERSITY PRESS
New Haven & London
To Pamela and Griffin, with love

Copyright © 2011 by Daniel J. Solove.
All rights reserved.
This book may not be reproduced, in whole or in part, including illustrations,
in any form (beyond that copying permitted by Sections 107 and 108 of the U.S.
Copyright Law and except by reviewers for the public press), without written
permission from the publishers.

Yale University Press books may be purchased in quantity for educational, business,
or promotional use. For information, please e-mail sales.press@yale.edu (U.S. office)
or sales@yaleup.co.uk (U.K. office).

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.
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

Contents

Preface vii

1 Introduction 1

PART I: Values: How We Should Assess and Balance the Values of Privacy and Security

2 The Nothing-to-Hide Argument 21

3 The All-or-Nothing Fallacy 33

4 The Danger of Deference 38

5 Why Privacy Isn't Merely an Individual Right 47

PART II: Times of Crisis: How the Law Should Address Matters of National Security

6 The Pendulum Argument 55

7 The National-Security Argument 62

8 The Problem with Dissolving the Crime-Espionage Distinction 71

9 The War-Powers Argument and the Rule of Law 81
## 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 mis impressions 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-
arguments 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.
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

<table>
<thead>
<tr>
<th>Year</th>
<th>Agents</th>
<th>Support Staff</th>
</tr>
</thead>
<tbody>
<tr>
<td>1933</td>
<td>353</td>
<td>422</td>
</tr>
<tr>
<td>1945</td>
<td>4,380</td>
<td>7,422</td>
</tr>
<tr>
<td>2008</td>
<td>12,705</td>
<td>17,871</td>
</tr>
</tbody>
</table>

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: "Sublimer 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 "confessed, 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


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-
bers of Congress had feared Hoover and declined to take him on, but a few years after his death, Congress finally decided to take a closer look at the FBI, an inquiry spurred by the Watergate scandal and President Nixon’s abuses of surveillance. Watergate involved electronic surveillance—the Watergate Office Building was burglarized in order to bug the phone of the Democratic Party chairman. Some of the charges in Nixon’s impending impeachment involved misuse of officials at the FBI, the Secret Service, and other agencies to conduct electronic surveillance for improper purposes.

After Nixon resigned, on August 9, 1974, Congress realized that it needed to examine more thoroughly the way various government agencies were engaging in surveillance. Congress formed a special eleven-member committee in 1975 to investigate surveillance abuses over the previous forty years.\(^{28}\) Led by Senator Frank Church, the committee published fourteen volumes of reports and supporting documents. The Church Committee concluded that the government had engaged in numerous abuses of surveillance, often targeting people solely because of their political beliefs. Specifically, the committee declared: “Too many people have been spied upon by too many Government agencies and [too] much information has [been] collected. The Government has often undertaken the secret surveillance of citizens on the basis of their political beliefs, even when those beliefs posed no threat of violence or illegal acts on behalf of a hostile foreign power.”\(^{29}\) As the committee noted, every president from Franklin Roosevelt to Richard Nixon improperly used government surveillance to obtain information about critics and political opponents.\(^{30}\)

In part as a response to shocking findings of the Church Committee Report, Congress passed the Foreign Intelligence Surveillance Act (FISA) in 1978.\(^{31}\) The purpose of FISA was to erect a “secure framework by which the executive branch could conduct legitimate electronic surveillance for foreign intelligence purposes within the context of this Nation’s commitment to privacy and individual rights.”\(^{32}\) Additionally, the attorney general established a set of guidelines for FBI investigations in 1976.\(^{33}\) Moreover, major reforms were instituted at the FBI to prevent the kinds of abuses that had occurred during Hoover’s reign as director. The FBI director was limited to a term of no longer than ten years.

**Receding Fourth Amendment Protection and the Rise of the Information Age**

In the 1970s and 1980s the Supreme Court issued several decisions narrowing the scope of Fourth Amendment protection. For example, the Court concluded that there was no reasonable expectation of privacy when the police obtained a list of the phone numbers a person dialed or gathered a person’s bank records or peered down on a person’s property from a helicopter or rummaged through a person’s trash left out for collection.\(^{34}\)

During the 1990s the rise of computers, the burgeoning use of the Internet and email, and the increasing use of digital records began to pose severe challenges for the federal wiretap statute, which had not been created with these new technologies in mind. In anticipation of the increasing use of computers, Congress updated its electronic surveillance law in 1986 with a statute called the Electronic Communications Privacy Act (ECPA).\(^{35}\) This law aimed to provide protection of email, stored computer files, and communications records. Unfortunately, the law has not been dramatically restructured since its passage. Changes have been made here and there, but the ECPA remains largely the same. A quarter of a century after its passage, it has gone far out of date.

**The War on Terrorism**

Then came the terrorist attacks of September 11, 2001. We became aware of dangerous terrorist cells within our borders. In an
extremely short time following the September 11 attacks, Congress passed the USA Patriot Act of 2001, which made a series of updates to ECPA and FISA, generally giving the government greater power to engage in surveillance. To better facilitate information sharing among the various federal agencies, many agencies were merged into DHS.

Throughout this time, the government engaged in many clandestine information-gathering programs. The NSA began wiretapping phone calls between U.S. citizens and people abroad. Various federal agencies collected records from airlines and other businesses for use in data mining.

Privacy, Security, and the Law

Throughout the past century, as we moved into the Information Age, the government has expanded its arsenal of techniques to protect security. Law enforcement in the past mostly involved searches of homes, people, and papers. Now the government uses technology to gather records and data, to engage in audio and visual surveillance, and to track movement. Much law-enforcement activity with implications for privacy involves “information gathering.” I’ll use this term broadly to encompass the wide variety of ways the government can find out what people are doing, thinking, or planning. In addition to gathering information, the government also stores it, uses it, analyzes it, combines it, and sometimes discloses it. All these activities can threaten privacy.

As the history I have sketched illustrates, the law has responded in many ways to the clash between privacy and security. Today the government has tremendous power and technological capabilities to enforce the law and promote security. The law establishes privacy protections to ensure that the government doesn’t abuse its power. The Fourth Amendment to the U.S. Constitution is the primary form of regulation of government information gathering.

Under our system of law, the Constitution provides the minimum level of privacy protection. A state can’t provide any less protection. Nor can a federal statute. Other amendments, such as the Fifth and (as I’ll argue later) the First, protect some dimensions of privacy.

In addition to the Constitution, several federal laws regulate certain forms of government information gathering. ECPA regulates wiretapping, bugging, and searches of computers, among other things. FISA regulates foreign intelligence gathering on foreign agents on U.S. soil. Other statutes provide some regulation of government access to our records, such as cable or health records.

There are also state constitutional protections of privacy and state statutes. These can supply additional privacy protections, though they restrict only police departments within a particular state. They can’t limit FBI agents or any other federal law-enforcement officials even when they’re acting within the state. Federal agents are limited only by the U.S. Constitution and federal statutes. In this book, my focus will be almost entirely on the U.S. Constitution and federal law.

Does the law provide a good balance between privacy and security? I believe the answer is no. Lessons learned after previous surveillance abuses have been forgotten. Protections put into the law in response to these abuses have been removed. I’ll explain how the law regulating privacy and security works, point out its failings, and suggest how it can be improved.

A Roadmap

In this book I shall explore four general issues, and I have organized it accordingly, devoting the four parts to (1) values—how we should assess and balance the values of privacy and security; (2) times of crisis—how the law should address matters of national security; (3) constitutional rights—how the Constitution should protect privacy; and (4) new technologies—how the law should cope with changing technology.
Within each part are chapters exploring various subtopics. You can read chapters independently of one another.

Values

Part I involves the values of privacy and security. How should we assess and understand these values? Can they be reconciled? How should we balance them when they conflict? The chapters in this part are concerned with how we can better understand what privacy protection entails, how we can more thoughtfully evaluate the costs and benefits of security measures, and how we can balance privacy and security in a way that isn’t skewed too much toward security. Privacy is often misunderstood and undervalued when balanced against security. It is possible to have potent security measures and to protect privacy too, since protecting privacy doesn’t entail scrapping security measures but demands only that they be subjected to oversight and regulation.

In Chapter 2 I examine the nothing-to-hide argument. Those making this common argument contend that they have nothing to hide from the government. I demonstrate why this argument is faulty.

Chapter 3 tackles another argument, that in order to increase security, we must sacrifice privacy. I call this the all-or-nothing fallacy because it falsely assumes that privacy and security are mutually exclusive.

In Chapter 4 I explore the deference argument—that we should be careful about second-guessing the judgments of security officials because they have more expertise in dealing with national security than judges or legislators. Courts often defer to security officials, and I argue that this deference unduly skews the balance between privacy rights and security.

In Chapter 5 I argue that privacy isn’t merely an individual right. The balancing between security and privacy is often conducted improperly because the security interest is characterized as beneficial for all society while the privacy interest is viewed as a particular individual’s concern. I contend that privacy should be understood as a societal value.

Times of Crisis

In Part II I examine the law during periods of crisis. When we’re facing a threat to national security, the government frequently curtails rights, circumvents laws, and demands greater discretion, more secrecy, and less oversight. The chapters in this part demonstrate that these special powers and exceptions to the rule of law are often unnecessary and wrongheaded.

In Chapter 6 I address the pendulum argument—that in times of crisis, we must sacrifice some liberties, which will be restored when the crisis is over. I contend that this argument has it exactly backward. In times of crisis, we should be at our staunchest in protecting liberty.

In Chapter 7 I critique the national security argument—that government information gathering about U.S. citizens in the name of national security should be subjected to less regulation and oversight than the investigation of ordinary crime. I argue that the distinction between matters of national security and regular crime is fuzzy and incoherent.

In Chapter 8 I discuss the importance of crime-espionage distinction—separating the rules regulating criminal investigation from the rules regulating espionage. After September 11, the distinction was significantly dissolved. I argue that the distinction must be kept intact.

In Chapter 9 I examine how law protecting privacy and other civil liberties is often violated in times of crisis. A prime example was
the NSA surveillance program, under which the NSA contravened the
law by engaging in warrantless wiretapping of phone calls. If we can't
ensure that the law is followed, the rule of law becomes meaningless.

Constitutional Rights

Part III focuses on constitutional rights. What do our constitutional rights entail? How do they protect us? Frequently, people think
that constitutional rights protect a lot more than they actually do. As I
explain in this part, numerous government information-gathering activities are completely unregulated. If the Constitution is to provide
for meaningful regulation and oversight of government data gathering in the Information Age, then the Supreme Court's interpretations of the Constitution need a radical overhaul.

In Chapter 10 I discuss the latest tools of government information gathering, many of which aren't restricted by the Fourth Amendment. The scope of Fourth Amendment regulation, which depends on whether the government violates privacy, is unduly constrained because the U.S. Supreme Court understands privacy as a form of total secrecy. I call this view of privacy the "secrecy paradigm," and I demonstrate that it is antiquated and flawed.

In Chapter 11 I analyze the "third party doctrine," which holds that whenever a person or business exposes information to another entity, no reasonable expectation of privacy remains, and thus no Fourth Amendment protection applies. In the Information Age, however, an unprecedented amount of personal data is in the hands of third parties, effectively removing Fourth Amendment protection from it.

In Chapter 12 I argue that Fourth Amendment law needs dramatic reform. In many cases, government activities are unregulated because the Supreme Court doesn't think "privacy" is involved. I propose that paradoxically the Fourth Amendment law would do a better job of protecting privacy by no longer focusing on privacy.

In Chapter 13 I explain the "suspicionless-searches" argument, which contends that requiring law enforcements to establish suspicion before engaging in a search isn't compatible with efforts to prevent terrorism. I show that abandoning the suspicion requirement—as embodied in warrants and probable cause—provides law-enforcement officials with too much power and discretion and too little oversight.

In Chapter 14 I examine whether the exclusionary rule, which makes evidence gathered in violation of the Fourth Amendment unusable at trial—is an appropriate remedy, especially when a heinous crime or terrorist act is involved. I discuss how the Fourth Amendment can be enforced without the exclusionary rule.

In Chapter 15 I argue that the First Amendment should protect you when the government seeks information about your speech, association, beliefs, or reading habits.

New Technologies

Part IV is concerned with the challenges that new technologies pose for the law. How should the law cope in a world of rapidly changing technology? In this part I examine the ways statutory law regulates government information gathering and the difficulty of keeping statutes up-to-date. The best way to protect privacy is never to lose sight of general principles. To avoid becoming outdated when the technology evolves, laws should be built around general principles rather than specific technologies.

In Chapter 16 I focus on the Patriot Act, a law many argue should be repealed. But what if the Patriot Act were to simply disappear tomorrow? Contrary to the conventional wisdom, little would change.

In Chapter 17 I critique the "leave-it-to-the-legislature argument"—that legislatures are better than courts at making the rules when new technologies are involved. I argue that courts must
Introduction

remain actively involved in order to ensure that the law keeps up with new technology.

In Chapter 18 I examine government data mining—the use of databases of personal information to analyze for patterns to determine who is acting suspiciously. Currently, the Fourth Amendment does not do much to protect against data mining. I distinguish between when the government should be allowed to engage in data mining and when it shouldn’t.

In Chapter 19 I argue that the law doesn’t adequately regulate public video surveillance. In the United Kingdom millions of surveillance cameras watch everything people do. Such a system could readily be implemented in America—and it currently is being implemented in various cities. I explain how the law can provide better regulation.

In Chapter 20 I critique the “Luddite argument”—that opposition to new security technologies (such as biometric identification) stems from an aversion to new technology. I argue that concerns about these technologies are often legitimate. While many of the technologies offer great upsides, they can have catastrophic consequences if they fail.

PART I

Values

How We Should Assess and Balance the Values of Privacy and Security
The Nothing-to-Hide Argument

When the government gathers or analyzes personal information, many people say they're not worried. “I've got nothing to hide,” they declare. “Only if you're doing something wrong should you worry, and then you don’t deserve to keep it private.”

The nothing-to-hide argument pervades discussions about privacy. The data security expert Bruce Schneier calls it the “most common retort against privacy advocates.” The legal scholar Geoffrey Stone refers to it as an “all-too-common refrain.” In its most compelling form, it is an argument that the privacy interest is generally minimal, thus making the balance against security concerns a foreordained victory for security. In this chapter, I'll demonstrate how the argument stems from certain faulty assumptions about privacy and its value.

“I've Got Nothing to Hide”

The nothing-to-hide argument is everywhere. In Britain, for example, the government has installed millions of public surveillance cameras in cities and towns, which are watched by officials via closed-circuit television. In a campaign slogan for the program, the government
declares: “If you’ve got nothing to hide, you’ve got nothing to fear.”3 In the United States, one anonymous individual comments: “If [government officials] need to read my e-mails . . . so be it. I have nothing to hide. Do you?”4 Variations of nothing-to-hide arguments frequently appear in blogs, letters to the editor, television news interviews, and other forums. One blogger, in reference to profiling people for national security purposes, declares: “Go ahead and profile me, I have nothing to hide.”5 Another blogger proclaims: “So I don’t mind people wanting to find out things about me, I’ve got nothing to hide! Which is why I support [the government’s] efforts to find terrorists by monitoring our phone calls!”6 Some other examples include:

- I don’t have anything to hide from the government. I don’t think I had that much hidden from the government in the first place. I don’t think they care if I talk about my ornery neighbor.7
- Do I care if the FBI monitors my phone calls? I have nothing to hide. Neither does 99.99 percent of the population. If the wiretapping stops one of these Sept. 11 incidents, thousands of lives are saved.8
- Like I said, I have nothing to hide. The majority of the American people have nothing to hide. And those that have something to hide should be found out, and get what they have coming to them.9

The nothing-to-hide argument is not of recent vintage. One of the characters in Henry James’s 1888 novel The Reverberator muses: "If these people had done bad things they ought to be ashamed of themselves and he couldn’t pity them, and if they hadn’t done them there was no need of making such a rumpus about other people knowing."10

I encountered the nothing-to-hide argument so frequently in news interviews, discussions, and the like that I decided to probe the issue. I asked the readers of my blog, Concurring Opinions, whether there are good responses to the nothing-to-hide argument.11 I received a torrent of comments:

- My response is “So do you have curtains?” or “Can I see your credit card bills for the last year?”
- So my response to the “If you have nothing to hide . . .” argument is simply, “I don’t need to justify my position. You need to justify yours. Come back with a warrant.”
- I don’t have anything to hide. But I don’t have anything I feel like showing you, either.
- If you have nothing to hide, then you don’t have a life.
- Show me yours and I’ll show you mine.
- It’s not about having anything to hide, it’s about things not being anyone else’s business.
- Bottom line, Joe Stalin would [have] loved it. Why should anyone have to say more?12

On the surface it seems easy to dismiss the nothing-to-hide argument. Everybody probably has something to hide from somebody. As the author Aleksandr Solzhenitsyn declared, “Everyone is guilty of something or has something to conceal. All one has to do is look hard enough to find what it is.”13 Likewise, in Friedrich Dürrenmatt’s novella Traps, which involves a seemingly innocent man put on trial by a group of retired lawyers for a mock trial game, the man inquires what his crime shall be. “An altogether minor matter,” the prosecutor replied. “A crime can always be found.”14

One can usually think of something that even the most open person would want to hide. As a commenter to my blog post noted, “If you have nothing to hide, then that quite literally means you are willing to let me photograph you naked? And I get full rights to that photograph—so I can show it to your neighbors?”15 The Canadian privacy expert David Flaherty expresses a similar idea when he argues: “There is no sentient human being in the Western world who has little or no regard for his or her personal privacy; those who would attempt such claims cannot withstand even a few minutes’ question-
Values

The Nothing-to-Hide Argument

Such responses attack the nothing-to-hide argument only in its most extreme form, which isn’t particularly strong. In a less extreme form, the nothing-to-hide argument refers not to all personal information but only to the type of data the government is likely to collect. Retorts to the nothing-to-hide argument about exposing people’s naked bodies or their deepest secrets are relevant only if the government is likely to gather this kind of information. In many instances, hardly anyone will see the information, and it won’t be disclosed to the public. Thus, some might argue, the privacy interest is minimal, and the security interest in preventing terrorism is much more important. In this less extreme form, the nothing-to-hide argument is a formidable one.

Understanding Privacy

To evaluate the nothing-to-hide argument, we should begin by looking at how its adherents understand privacy. Nearly every law or policy involving privacy depends upon a particular understanding of what privacy is. The way problems are conceived has a tremendous impact on the legal and policy solutions used to solve them. As the philosopher John Dewey observed, “A problem well put is half-solved.”

What is “privacy”? Most attempts to understand privacy do so by attempting to locate the essence of privacy — its core characteristics or the common denominator that links together the various things we classify under the rubric of “privacy.” Privacy, however, is too complex a concept to be reduced to a singular essence. It is a plurality of different things that do not share one element in common but that nevertheless bear a resemblance to each other. For example, privacy can be invaded by the disclosure of your deepest secrets. It might also be invaded if you’re watched by a Peeping Tom, even if no secrets are ever revealed to anyone. With the disclosure of secrets, the harm is that your concealed information is spread to others. With the Peeping Tom, the harm is that you’re being watched. You’d probably find it creepy regardless of whether the peeper finds out anything sensitive or discloses any information to others.

There are many other forms of invasion of privacy, such as blackmail or the improper use of your personal data. Your privacy can also be invaded if the government compiles an extensive dossier about you. Privacy thus involves so many different things that it is impossible to reduce them all to one simple idea. We need not do so.

In many cases, privacy issues never get balanced against conflicting interests because courts, legislators, and others fail to recognize that privacy is implicated. People don’t acknowledge certain problems because they don’t fit into their particular one-size-fits-all conception of privacy. Regardless of whether we call something a “privacy” problem, it still remains a problem, and problems shouldn’t be ignored. We should pay attention to all the different problems that spark our desire to protect privacy.

To describe the problems created by the collection and use of personal data, many commentators use a metaphor based on George Orwell’s Nineteen Eighty-Four. Orwell depicted a harrowing totalitarian society ruled by a government called Big Brother that watched its citizens obsessively and demanded strict discipline. The Orwell metaphor, which focuses on the harms of surveillance (such as inhibition and social control), might be apt to describe government monitoring of citizens. But much of the data gathered in computer databases isn’t particularly sensitive, such as one’s race, birth date, gender, address, or marital status. Many people don’t care about concealing the hotels they stay at, the cars they own, or the kind of beverages they drink. Frequently, though not always, people wouldn’t be inhibited or embarrassed if others knew this information.
A different metaphor better captures the problems: Franz Kafka's *The Trial*. Kafka's novel centers around a man who is arrested but not informed why. He desperately tries to find out what triggered his arrest and what's in store for him. He finds out that a mysterious court system has a dossier on him and is investigating him, but he's unable to learn much more. *The Trial* depicts a bureaucracy with inscrutable purposes that uses people's information to make important decisions about them, yet denies the people the ability to participate in how their information is used. The problems portrayed by the Kafkaesque metaphor are of a different sort from the problems caused by surveillance. They often do not result in inhibition. Instead, they are problems of information processing—the storage, use, or analysis of data—rather than of information collection. They affect the power relationships between people and the institutions of the modern state. They not only frustrate the individual by creating a sense of helplessness and powerlessness, they also affect social structure by altering the kind of relationships people have with the institutions that make important decisions about their lives.

Legal and policy solutions focus too much on the problems under the Orwellian metaphor—those of surveillance—and aren't adequately addressing the Kafkaesque problems—those of information processing. The difficulty is that commentators are trying to conceive of the problems caused by databases in terms of surveillance when, in fact, these problems are different.

The Problem with the Nothing-to-Hide Argument

Commentators often attempt to refute the nothing-to-hide argument by pointing to things people want to hide. But the problem with the nothing-to-hide argument is the underlying assumption that privacy is about hiding bad things. By accepting this assumption we concede far too much ground and invite an unproductive discussion of information people would likely want to hide. As Bruce Schneier aptly notes, the nothing-to-hide argument stems from a faulty "premise that privacy is about hiding a wrong." Surveillance, for example, can inhibit such lawful activities as free speech, free association, and other First Amendment rights essential for democracy.

The deeper problem with the nothing-to-hide argument is that it myopically views privacy as a form of secrecy. In contrast, understanding privacy as a plurality of related issues demonstrates that the disclosure of bad things is just one among many difficulties caused by government security measures. To return to my discussion of literary metaphors, the problems are not just Orwellian but Kafkaesque. Government information-gathering programs are problematic even if no information people want to hide is uncovered. In *The Trial*, the problem is not inhibited behavior but rather a suffocating powerlessness and vulnerability created by the court system's use of personal data and its denial to the protagonist of any knowledge of or participation in the process. The harms are bureaucratic ones—indifference, error, abuse, frustration, and lack of transparency and accountability.

One such harm, for example, which I call *exclusion*, emerges from the fusion of small bits of seemingly innocuous data. When combined, the information becomes much more telling. By joining pieces of information we might not take pains to guard, the government can glean information about us that we might indeed wish to conceal. For example, suppose you bought a book about cancer. This purchase isn't very revealing on its own, for it just indicates an interest in the disease. Suppose you bought a wig. The purchase of a wig, by itself, could be for a number of reasons. But combine these two pieces of information, and now the inference can be made that you have cancer and are undergoing chemotherapy.

Another potential problem with the government's harvest of personal data is one I call *exclusion*. Exclusion occurs when people are prevented from having knowledge about how information about
them is being used, and when they are barred from accessing and correcting errors in that data. Many government national security measures involve maintaining a massive database of information that individuals cannot access. Indeed, because they involve national security, the very existence of these programs is often kept secret. This kind of information processing, which blocks subjects’ knowledge and involvement, resembles in some ways a kind of due-process problem. It is a structural problem involving the way people are treated by government institutions and creating a power imbalance between individuals and the government. To what extent should government officials have such a significant power over citizens? This issue isn’t about what information people want to hide but about the power and the structure of government.

A related problem involves secondary use. Secondary use is the exploitation of data obtained for one purpose for an unrelated purpose without the subject’s consent. How long will personal data be stored? How will it be used? What could it be used for in the future? The potential future uses of any piece of personal information are vast, and without limits on or accountability for how that information is used, it is hard for people to assess the dangers of the data’s being in the government’s control.

Yet another problem with government gathering and use of personal data is distortion. Although personal information can reveal quite a lot about people’s personalities and activities, it often fails to reflect the whole person. It can paint a distorted picture, especially since records are reductive—they often capture information in a standardized format with many details omitted.

For example, suppose government officials learn that a person has bought a number of books on how to manufacture methamphetamine. That information makes them suspect that he’s building a meth lab. What is missing from the records is the full story: The person is writing a novel about a character who makes meth. When he bought the books, he didn’t consider how suspicious the purchase

might appear to government officials, and his records didn’t reveal the reason for the purchases. Should he have to worry about government scrutiny of all his purchases and actions? Should he have to be concerned that he’ll wind up on a suspicious-persons list? Even if he isn’t doing anything wrong, he may want to keep his records away from government officials who might make faulty inferences from them. He might not want to have to worry about how everything he does will be perceived by officials nervously monitoring for criminal activity. He might not want to have a computer flag him as suspicious because he has an unusual pattern of behavior.

The problem with the nothing-to-hide argument is that it focuses on just one or two particular kinds of privacy problems—the disclosure of personal information or surveillance—while ignoring others. It assumes a particular view about what privacy entails to the exclusion of other perspectives.

It is important to distinguish here between two ways of justifying a national security program that demands access to personal information. The first way is not to recognize a problem. This is how the nothing-to-hide argument works—it denies even the existence of a problem. The second manner of justifying such a program is to acknowledge the problems but contend that the benefits of the program outweigh the privacy sacrifice. The first justification influences the second, because the low value given to privacy is based upon a narrow view of the problem. The key misunderstanding is that the nothing-to-hide argument views privacy in a particular way—as a form of secrecy, as the right to hide things. But there are many other types of harm involved beyond exposing one’s secrets to the government.

Blood, Death, and Privacy

One of the difficulties with the nothing-to-hide argument is that it looks for a singular and visceral kind of injury. Ironically, this underly-
ing conception of injury is sometimes shared by those advocating for greater privacy protections. For example, the law professor Ann Bartow argues that in order to have a real resonance, privacy problems must “negatively impact the lives of living, breathing human beings beyond simply provoking feelings of unease.” She urges that privacy needs more “dead bodies” and that privacy’s “lack of blood and death, or at least of broken bones and buckets of money, distances privacy harms from other [types of harm].”

Bartow’s objection is actually consistent with the nothing-to-hide argument. Those advancing the nothing-to-hide argument have in mind a particular kind of appalling privacy harm, one where privacy is violated only when something deeply embarrassing or discrediting is revealed. Like Bartow, proponents of the nothing-to-hide argument demand a dead-bodies type of harm.

Bartow is certainly right that people respond much more strongly to blood and death than to more abstract concerns. But if this is the standard to recognize a problem, then few privacy problems will be recognized. Privacy is not a horror movie, most privacy problems don’t result in dead bodies, and demanding more palpable harms will be difficult in many cases.

In many instances, privacy is threatened not by a single egregious act but by the accretion of a slow series of relatively minor acts. In this respect, privacy problems resemble certain environmental harms which occur over time through a series of small acts by different actors. Although society is more likely to respond to a major oil spill, gradual pollution by a multitude of different actors often creates worse problems.

Privacy is rarely lost in one fell swoop. It is often eroded over time, little bits dissolving almost imperceptibly until we finally begin to notice how much is gone. When the government starts monitoring the phone numbers people call, many may shrug their shoulders and say, “Ah, it’s just numbers, that’s all.” Then the government might start monitoring some phone calls. “It’s just a few phone calls, noth-

ing more,” people might declare. The government might install more video cameras in public places, to which some would respond, “So what? Some more cameras watching in a few more places. No big deal.” The increase in cameras might ultimately expand to a more elaborate network of video surveillance. Satellite surveillance might be added, as well as the tracking of people’s movements. The government might start analyzing people’s bank records. “It’s just my deposits and some of the bills I pay—no problem.” The government may then start combing through credit card records, then expand to Internet service provider (ISP) records, health records, employment records, and more. Each step may seem incremental, but after a while, the government will be watching and knowing everything about us.

“My life’s an open book,” people might say. “I’ve got nothing to hide.” But now the government has a massive dossier of everyone’s activities, interests, reading habits, finances, and health. What if the government leaks the information to the public? What if the government mistakenly determines that based on your pattern of activities, you’re likely to engage in a criminal act? What if it denies you the right to fly? What if the government thinks your financial transactions look odd—even if you’ve done nothing wrong—and freezes your accounts? What if the government doesn’t protect your information with adequate security, and an identity thief obtains it and uses it to defraud you? Even if you have nothing to hide, the government can cause you a lot of harm.

“But the government doesn’t want to hurt me,” some might argue. In many cases, this is true, but the government can also harm people inadvertently, due to errors or carelessness.

Silencing the Nothing-to-Hide Argument

When the nothing-to-hide argument is unpacked, and its underlying assumptions examined and challenged, we can see how it shifts the
debate to its terms, then draws power from its unfair advantage. The nothing-to-hide argument speaks to some problems, but not to others. It represents a singular and narrow way of conceiving of privacy, and it wins by excluding consideration of the other problems often raised with government security measures. When engaged directly, the nothing-to-hide argument can ensnare, for it forces the debate to focus on its narrow understanding of privacy. But when confronted with the plurality of privacy problems implicated by government data collection and use beyond surveillance and disclosure, the nothing-to-hide argument, in the end, has nothing to say.

The All-or-Nothing Fallacy

I'd gladly give up my privacy if it will keep me secure from a terrorist attack.” I hear this refrain again and again. The debate is often cast as an all-or-nothing choice, whether we should have privacy or a specific security measure. Consider the way the government defended the NSA surveillance program, which involved secret wiretapping of phone calls without any oversight. In a congressional hearing, Attorney General Alberto Gonzales stated: “Our enemy is listening, and I cannot help but wonder if they are not shaking their heads in amazement at the thought that anyone would imperil such a sensitive program by leaking its existence in the first place, and smiling at the prospect that we might now disclose even more or perhaps even unilaterally disarm ourselves of a key tool in the war on terror.”

Notice his language. He’s implying that if we protect privacy, it will mean that we must “disarm” ourselves of some really valuable security measures. He’s suggesting that even terrorists would consider us crazy for making such a tradeoff.

I constantly hear arguments like this when officials justify security measures or argue that they shouldn’t be regulated. They point to the value of the surveillance and the peril we’d be in without it. “We’re hearing quite a lot of chatter about terrorist attacks,” they say.
forgets about the problems it must solve and the core principles it must promote.

So let the debate begin anew, but let it be more productive this time. Let's finally make some headway. If we get rid of all the noise and confusion, we can focus on what works and what doesn't. We can come to meaningful compromises. We can protect privacy as well as have effective security.

\[210\]

\[211\]

2. The Nothing-to-Hide Argument

16. David H. Flaherty, Visions of Privacy: Past, Present, in
3. The All-or-Nothing Fallacy


4. The Danger of Deference


5. See id. at 6, 31, 18.

6. JOHN MUELLER, OVERBLOWN: HOW POLITICIANS AND THE TERRORISM

7. See BRUCE SCHNEIER, BEYOND FEAR: THINKING SENSIBLY ABOUT SECURITY IN AN UNCERTAIN WORLD 239 (2003).


5. Why Privacy Isn’t Merely an Individual Right


3. Charles Fried, Privacy, 77 YALE L.J. 475, 478 (1968); see also BEATE RÖSSLER, THE VALUE OF PRIVACY 117 (R. D. V. Glasgow trans., 2005) (“Respect for a person’s privacy is respect for her as an autonomous subject.”); Stanley L. Benn, Privacy, Freedom, and Respect for Persons, in NOMOS XIII: PRIVACY 1, 26 (J. Roland Pennock & John W. Chapman eds., 1971) (“[R]espect for someone as a person, as a chooser, implies[ ] respect for him as one engaged in a kind of self-creative enterprise, which could be disrupted, distorted, or frustrated even by so limited an intrusion as watching.”).


6. Id. at 198.


10. Spiros Simitis, Reviewing Privacy in an Information Society, 135 U. PA. L. REV. 707, 709 (1987) (“[P]rivacy considerations no longer arise out of particular individual problems; rather, they express conflicts affecting everyone.”); see also