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

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.
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

Contents

2

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."[1] The legal scholar Geoffrey Stone refers to it as an "all-too-common refrain."[2] 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-

ing about intimate aspects of their lives without capitulating to the intrusiveness of certain subject matters."[16]

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."[17]

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.[18] 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*.[19] 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.[20] 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.[21] 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 informa-

tion 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."[22] 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 *aggregation*, 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]."[23]

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.