"I've Got Nothing to Hide" and Other Misunderstandings of Privacy

DANIEL J. SOLOVE*

TABLE OF CONTENTS

I. INTRODUCTION

Since the September 11 attacks, the government has been engaging in extensive surveillance and data mining. Regarding surveillance, in December 2005, the *New York Times* revealed that after September 11, the Bush Administration secretly authorized the National Security Administration (NSA) to engage in warrantless wiretapping of American citizens' telephone calls.[1] As for data mining, which involves analyzing

 Associate Professor, George Washington University Law School; J.D., Yale Law School. Thanks to Chris Hoofnagle, Adam Moore, and Michael Sullivan for helpful comments, and to my research assistant Sheerin Shahinpoor. I develop some of the ideas in this essay in significantly more depth in my forthcoming book, *Understanding Privacy*, to be published by Harvard University Press in May 2008.

1. James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts: Secret Order to Widen Domestic Monitoring*, N.Y. TIMES, Dec. 16, 2005, at A1.

personal data for patterns of suspicious behavior, the government has begun numerous programs. In 2002, the media revealed that the Department of Defense was constructing a data mining project, called "Total Information Awareness" (TIA), under the leadership of Admiral John Poindexter.[2] The vision for TIA was to gather a variety of information about people, including financial, educational, health, and other data. The information would then be analyzed for suspicious behavior patterns. According to Poindexter: "The only way to detect . . . terrorists is to look for patterns of activity that are based on observations from past terrorist attacks as well as estimates about how terrorists will adapt to our measures to avoid detection."[3] When the program came to light, a public outcry erupted, and the U.S. Senate subsequently voted to deny the program funding, ultimately leading to its demise.[4] Nevertheless, many components of TIA continue on in various government agencies, though in a less systematic and more clandestine fashion.[5]

In May 2006, *USA Today* broke the story that the NSA had obtained customer records from several major phone companies and was analyzing them to identify potential terrorists.[6] The telephone call database is reported to be the "largest database ever assembled in the world."[7] In June 2006, the *New York Times* stated that the U.S. government had been accessing bank records from the Society for Worldwide Interbank Financial Transactions (SWIFT), which handles financial transactions for thousands of banks around the world.[8] Many people responded with outrage at these announcements, but many others did not perceive much of a problem. The reason for their lack of concern, they explained, was because: "I've got nothing to hide."[9]

The argument that no privacy problem exists if a person has nothing to hide is frequently made in connection with many privacy issues. When the government engages in surveillance, many people believe that there is no threat to privacy unless the government uncovers unlawful activity, in which case a person has no legitimate justification to claim that it

2. John Markoff, *Pentagon Plans a Computer System That Would Peek at Personal Data of Americans*, N.Y. TIMES, Nov. 9, 2002, at A12.

3. John M. Poindexter, *Finding the Face of Terror in Data*, N.Y. TIMES, Sept. 10, 2003, at A25.

4. DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 169 (2004).

5. Shane Harris, *TIA Lives On*, NAT'L J., Feb. 25, 2006, at 66.

6. Leslie Cauley, *NSA Has Massive Database of Americans' Phone Calls*, USA TODAY, May 11, 2006, at A1; Susan Page, *Lawmakers: NSA Database Incomplete*, USA TODAY, June 30, 2006, at A1.

7. Cauley, *supra* note 6, at A1.

8. Eric Lichtblau & James Risen, *Bank Data Sifted in Secret by U.S. to Block Terror*, N.Y. TIMES, June 23, 2006, at A1.

9. *See infra* text accompanying notes 12–33.

remain private. Thus, if an individual engages only in legal activity, she has nothing to worry about. When it comes to the government collecting and analyzing personal information, many people contend that a privacy harm exists only if skeletons in the closet are revealed. For example, suppose the government examines one's telephone records and finds out that a person made calls to her parents, a friend in Canada, a video store, and a pizza delivery place. "So what?," that person might say. "I'm not embarrassed or humiliated by this information. If anybody asks me, I'll gladly tell them where I shop. I have nothing to hide."

The "nothing to hide" argument and its variants are quite prevalent in popular discourse about privacy. Data security expert Bruce Schneier calls it the "most common retort against privacy advocates."[10] Legal scholar Geoffrey Stone refers to it as "all-too-common refrain."[11] The nothing to hide argument is one of the primary arguments made when balancing privacy against security. In its most compelling form, it is an argument that the privacy interest is generally minimal to trivial, thus making the balance against security concerns a foreordained victory for security. Sometimes the nothing to hide argument is posed as a question: "If you have nothing to hide, then what do you have to fear?" Others ask: "If you aren't doing anything wrong, then what do you have to hide?"

In this essay, I will explore the nothing to hide argument and its variants in more depth. Grappling with the nothing to hide argument is important, because the argument reflects the sentiments of a wide percentage of the population. In popular discourse, the nothing to hide argument's superficial incantations can readily be refuted. But when the argument is made in its strongest form, it is far more formidable.

In order to respond to the nothing to hide argument, it is imperative that we have a theory about what privacy is and why it is valuable. At its core, the nothing to hide argument emerges from a conception of privacy and its value. What exactly is "privacy"? How valuable is privacy and how do we assess its value? How do we weigh privacy against countervailing values? These questions have long plagued those seeking to develop a theory of privacy and justifications for its legal protection.

10. Bruce Schneier, Commentary, *The Eternal Value of Privacy*, WIRED, May 18, 2006, http://www.wired.com/news/columns/1,70886-0.html.

11. Geoffrey R. Stone, Commentary, *Freedom and Public Responsibility*, CHI. TRIB., May 21, 2006, at 11.

This essay begins in Part II by discussing the nothing to hide argument. First, I introduce the argument as it often exists in popular discourse and examine frequent ways of responding to the argument. Second, I present the argument in what I believe to be its strongest form. In Part III, I briefly discuss my work thus far on conceptualizing privacy. I explain why existing theories of privacy have been unsatisfactory, have led to confusion, and have impeded the development of effective legal and policy responses to privacy problems. In Part IV, I argue that the nothing to hide argument—even in its strongest form—stems from certain faulty assumptions about privacy and its value. The problem, in short, is not with finding an answer to the question: "If you've got nothing to hide, then what do you have to fear?" The problem is in the very question itself.

II. THE "NOTHING TO HIDE" ARGUMENT

When discussing whether government surveillance and data mining pose a threat to privacy, many people respond that they have nothing to hide. This argument permeates the popular discourse about privacy and security issues. 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.[12] In a campaign slogan for the program, the government declares: "If you've got nothing to hide, you've got nothing to fear."[13] In the United States, one anonymous individual from the Department of Justice comments: "If [government officials] need to read my e-mails . . . so be it. I have nothing to hide. Do you?"[14] One blogger, in reference to profiling people for national security purposes, declares: "Go ahead and profile me, I have nothing to hide."[15] 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 President Bush's efforts to find terrorists by monitoring our phone calls!"[16] Variations of nothing to hide arguments frequently appear in blogs, letters to the editor, television news interviews, and other forums. Some examples include:

12. JEFFREY ROSEN, THE NAKED CROWD: RECLAIMING SECURITY AND FREEDOM IN AN ANXIOUS AGE (2004).

13. *Id.* at 36.

14. Comment of NonCryBaby to http://www.securityfocus.com/comments/articles/2296/18105/threaded (Feb. 12, 2003).

15. Comment of Yoven to http://www.danielpipes.org/comments/47675 (June 14, 2006, 14:03 EST).

16. Reach For The Stars!, http://greatcarrieoakey.blogspot.com/2006/05/look-all-you-want-ive-got-nothing-to.html (May 14, 2006, 09:04 PST).

- 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.[17]
- 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.[18]
- 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.[19]

The argument is not only of recent vintage. For example, one of the characters in Henry James's 1888 novel, *The Reverberator*, muses: "[I]f 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."[20]

I encountered the nothing to hide argument so frequently in news interviews, discussions, and the like, that I decided to blog about the issue. I asked the readers of my blog, *Concurring Opinions*, whether there are good responses to the nothing to hide argument.[21] I received a torrent of comments to my post:

- My response is "So do you have curtains?" or "Can I see your credit card bills for the last year?"[22]
- 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."[23]

17. Comment of annegb to Concurring Opinions, http://www.concurringopinions.com/archives/2006/05/is_there_a_good.html#comments (May 23, 2006, 11:37 EST).

18. Joe Schneider, Letter to the Editor, *NSA Wiretaps Necessary*, ST. PAUL PIONEER PRESS, Aug. 24, 2006, at 11B.

19. *Polls Suggest Americans Approve NSA Monitoring* (NPR radio broadcast, May 19, 2006), *available at* 2006 WLNR 22949347.

20. HENRY JAMES, THE REVERBERATOR (1888), *reprinted in* NOVELS 1886–1880, at 555, 687 (1989).

21. Concurring Opinions, *supra* note 17 (May 23, 2006, 00:06 EST).

22. Comment of Adam to Concurring Opinions, *supra* note 17 (May 23, 2006, 16:27 EST).

23. Comment of Dissent to Concurring Opinions, *supra* note 17 (May 24, 2006, 07:48 EST).

- I don't have anything to hide. But I don't have anything I feel like showing you, either.[24]
- If you have nothing to hide, then you don't have a life.[25]
- Show me yours and I'll show you mine.[26]
- It's not about having anything to hide, it's about things not being anyone else's business.[27]
- Bottom line, Joe Stalin would [have] loved it. Why should anyone have to say more?[28]

Most replies to the nothing to hide argument quickly respond with a witty retort. Indeed, 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."[29] 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.'"[30] One can usually think of something compelling that even the most open person would want to hide. As one comment 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?"[31] Canadian privacy expert David Flaherty expresses a similar idea when he argues:

24. Comment of Ian to Concurring Opinions, *supra* note 17 (May 24, 2006, 19:51 EST).
25. Comment of Matthew Graybosch to Concurring Opinions, *supra* note 17 (Oct. 16, 2006, 12:09 EST).
26. Comment of Neureaux to Concurring Opinions, *supra* note 17 (Oct. 16, 2006, 14:39 EST).
27. Comment of Catter to Concurring Opinions, *supra* note 17 (Oct. 16, 2006, 11:36 PM EST).
28. Comment of Kevin to Concurring Opinions, *supra* note 17 (July 24, 2006, 12:36 EST).
29. ALEKSANDR SOLZHENITSYN, CANCER WARD 192 (Nicholas Bethell & David Burg trans., Noonday Press 1991) (1968).
30. FRIEDRICH DÜRRENMATT, TRAPS 23 (Richard & Clara Winston trans., 1960).
31. Comment of Andrew to Concurring Opinions, *supra* note 17 (Oct. 16, 2006, 15:06 EST).

> 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' questioning about intimate aspects of their lives without capitulating to the intrusiveness of certain subject matters.[32]

Such responses only attack the nothing to hide argument in its most extreme form, which is not particularly strong. As merely a one-line utterance about a particular person's preference, the nothing to hide argument is not very compelling. But stated in a more sophisticated manner, the argument is more challenging. First, it must be broadened beyond the particular person making it. When phrased as an individual preference, the nothing to hide argument is hard to refute because it is difficult to quarrel with one particular person's preferences. As one commenter aptly notes:

> By saying "I have nothing to hide," you are saying that it's OK for the government to infringe on the rights of potentially millions of your fellow Americans, possibly ruining their lives in the process. To me, the "I have nothing to hide" argument basically equates to "I don't care what happens, so long as it doesn't happen to me."[33]

In its more compelling variants, the nothing to hide argument can be made in a more general manner. Instead of contending that "I've got nothing to hide," the argument can be recast as positing that all law-abiding citizens should have nothing to hide. Only if people desire to conceal unlawful activity should they be concerned, but according to the nothing to hide argument, people engaged in illegal conduct have no legitimate claim to maintaining the privacy of such activities.

In a related argument, Judge Richard Posner contends: "[W]hen people today decry lack of privacy, what they want, I think, is mainly something quite different from seclusion: they want more power to conceal information about themselves that others might use to their disadvantage."[34] Privacy involves a person's "right to conceal discreditable facts about himself."[35] In other words, privacy is likely to be invoked when there is something to hide and that something consists of negative

32. David H. Flaherty, *Visions of Privacy: Past, Present, and Future*, *in* VISIONS OF PRIVACY: POLICY CHOICES FOR THE DIGITAL AGE 19, 31 (Colin J. Bennett & Rebecca Grant eds., 1999).

33. Comment of BJ Horn to Concurring Opinions, *supra* note 17 (June 2, 2006, 18:58 EST).

34. RICHARD A. POSNER, THE ECONOMICS OF JUSTICE 271 (1983).

35. RICHARD A. POSNER, ECONOMIC ANALYSIS OF LAW 46 (5th ed. 1998).

information about a person. Posner asserts that the law should not protect people in concealing discreditable information. "The economist," he argues, "sees a parallel to the efforts of sellers to conceal defects in their products."[36]

Of course, one might object, there is nondiscreditable information about people that they nevertheless want to conceal because they find it embarrassing or just do not want others to know about. In a less extreme form, the nothing to hide argument does not refer to all personal information, but only to that subset of personal information that is likely to be involved in government surveillance. When people respond to NSA surveillance and data mining that they have nothing to hide, the more sophisticated way of understanding their argument should be as applying to the particular pieces of information that are gathered in the NSA programs. Information about what phone numbers people dial and even what they say in many conversations is often not likely to be embarrassing or discreditable to a law-abiding citizen. Retorts to the nothing to hide argument about exposing people's naked bodies to the world or revealing their deepest secrets to their friends are only relevant if there is a likelihood that such programs will actually result in these kinds of disclosures. This type of information is not likely to be captured in the government surveillance. Even if it were, many people might rationally assume that the information will be exposed only to a few law enforcement officials, and perhaps not even seen by human eyes. Computers might store the data and analyze it for patterns, but no person might have any contact with the data. As Posner argues:

> The collection, mainly through electronic means, of vast amounts of personal data is said to invade privacy. But machine collection and processing of data cannot, as such, invade privacy. Because of their volume, the data are first sifted by computers, which search for names, addresses, phone numbers, etc., that may have intelligence value. This initial sifting, far from invading privacy (a computer is not a sentient being), keeps most private data from being read by any intelligence officer.[37]

There is one final component of the most compelling versions of the nothing to hide argument—a comparison of the relative value of the privacy interest being threatened with the government interest in promoting security. As one commenter to my blog post astutely notes: "You can't talk about how people feel about the potential loss of privacy in any meaningful way without recognizing that most of the people who don't mind the NSA programs see it as a potential exchange of a small

36. *Id.*

37. Richard A. Posner, *Our Domestic Intelligence Crisis*, WASH. POST, Dec. 21, 2005, at A31.

amount of privacy for a potential national security gain."[38] In other words, the nothing to hide argument can be made by comparing the relative value between privacy and security. The value of privacy, the argument provides, is low, because the information is often not particularly sensitive. The ones with the most to worry about are the ones engaged in illegal conduct, and the value of protecting their privacy is low to nonexistent. On the government interest side of the balance, security has a very high value. Having a computer analyze the phone numbers one dials is not likely to expose deep dark secrets or embarrassing information to the world. The machine will simply move on, oblivious to any patterns that are not deemed suspicious. In other words, if you are not doing anything wrong, you have nothing to hide and nothing to fear.

Therefore, in a more compelling form than is often expressed in popular discourse, the nothing to hide argument proceeds as follows: The NSA surveillance, data mining, or other government information-gathering programs will result in the disclosure of particular pieces of information to a few government officials, or perhaps only to government computers. This very limited disclosure of the particular information involved is not likely to be threatening to the privacy of law-abiding citizens. Only those who are engaged in illegal activities have a reason to hide this information. Although there may be some cases in which the information might be sensitive or embarrassing to law-abiding citizens, the limited disclosure lessens the threat to privacy. Moreover, the security interest in detecting, investigating, and preventing terrorist attacks is very high and outweighs whatever minimal or moderate privacy interests law-abiding citizens may have in these particular pieces of information.

Cast in this manner, the nothing to hide argument is a formidable one. It balances the degree to which an individual's privacy is compromised by the limited disclosure of certain information against potent national security interests. Under such a balancing scheme, it is quite difficult for privacy to prevail.

38. Comment of MJ to Concurring Opinions, *supra* note 17 (May 23, 2006, 17:30 EST).

IV. THE PROBLEM WITH THE "NOTHING TO HIDE" ARGUMENT

A. Understanding the Many Dimensions of Privacy

It is time to return to the nothing to hide argument. The reasoning of this argument is that when it comes to government surveillance or use of personal data, there is no privacy violation if a person has nothing sensitive, embarrassing, or illegal to conceal. Criminals involved in illicit activities have something to fear, but for the vast majority of people, their activities are not illegal or embarrassing.

Understanding privacy as I have set forth reveals the flaw of the nothing to hide argument at its roots. Many commentators who respond to the argument attempt a direct refutation by trying to point to things that people would want to hide. But the problem with the nothing to hide argument is the underlying assumption that privacy is about hiding bad things. Agreeing with this assumption concedes far too much ground and leads to an unproductive discussion of information people would likely want or not 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."[75]

The deeper problem with the nothing to hide argument is that it myopically views privacy as a form of concealment or secrecy. But understanding privacy as a plurality of related problems demonstrates that concealment of bad things is just one among many problems caused by government programs such as the NSA surveillance and data mining. In the categories in my taxonomy, several problems are implicated.

The NSA programs involve problems of information collection, specifically the category of surveillance in the taxonomy. Wiretapping involves audio surveillance of people's conversations. Data mining often begins with the collection of personal information, usually from various third parties that possess people's data. Under current Supreme Court Fourth Amendment jurisprudence, when the government gathers data from third parties, there is no Fourth Amendment protection because people lack a "reasonable expectation of privacy" in information exposed to others.[76] In *United States v. Miller*, the Supreme Court concluded that there is no reasonable expectation of privacy in bank records because "[a]ll of the documents obtained, including financial statements and

75. Schneier, *supra* note 10.
76. United States v. Katz, 389 U.S. 347, 360–61 (1967) (Harlan, J., concurring).

deposit slips, contain only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business."[77] In *Smith v. Maryland*, the Supreme Court held that people lack a reasonable expectation of privacy in the phone numbers they dial because they "know that they must convey numerical information to the phone company," and therefore they cannot "harbor any general expectation that the numbers they dial will remain secret."[78] As I have argued extensively elsewhere, the lack of Fourth Amendment protection of third party records results in the government's ability to access an extensive amount of personal information with minimal limitation or oversight.[79]

Many scholars have referred to information collection as a form of surveillance. *Dataveillance*, a term coined by Roger Clarke, refers to the "systemic use of personal data systems in the investigation or monitoring of the actions or communications of one or more persons."[80] Christopher Slobogin has referred to the gathering of personal information in business records as "transaction surveillance."[81] Surveillance can create chilling effects on free speech, free association, and other First Amendment rights essential for democracy.[82] Even surveillance of legal activities can inhibit people from engaging in them. The value of protecting against chilling effects is not measured simply by focusing on the particular individuals who are deterred from exercising their rights. Chilling effects harm society because, among other things, they reduce the range of viewpoints expressed and the degree of freedom with which to engage in political activity.

The nothing to hide argument focuses primarily on the information collection problems associated with the NSA programs. It contends that limited surveillance of lawful activity will not chill behavior sufficiently to outweigh the security benefits. One can certainly quarrel with this

77. 425 U.S. 435, 442 (1976).
78. 442 U.S. 735, 743 (1979).
79. SOLOVE, *supra* note 4, at 165–209; *see also* Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083, 1117–37 (2002).
80. Roger Clarke, *Information Technology and Dataveillance*, 31 COMM. OF THE ACM 498, 499 (1988); *see also* Roger Clarke, *Introduction to Dataveillance and Information Privacy, and Definitions of Terms*, AUSTRALIAN NATIONAL UNIVERSITY, Aug. 7, 2006, http://www.anu.edu.au/people/Roger.Clarke/DV/Intro.html.
81. Christopher Slobogin, *Transaction Surveillance by the Government*, 75 MISS. L.J. 139, 140 (2005).
82. Daniel J. Solove, *The First Amendment as Criminal Procedure*, 82 N.Y.U. L. REV. 112, 154–59 (2007).

argument, but one of the difficulties with chilling effects is that it is often very hard to demonstrate concrete evidence of deterred behavior.[83] Whether the NSA's surveillance and collection of telephone records has deterred people from communicating particular ideas would be a difficult question to answer.

Far too often, discussions of the NSA surveillance and data mining define the problem solely in terms of surveillance. To return to my discussion of metaphor, the problems are not just Orwellian, but Kafkaesque. The NSA 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 exclusion of the protagonist from having any knowledge or participation in the process. The harms consist of those created by bureaucracies—indifference, errors, abuses, frustration, and lack of transparency and accountability. One such harm, for example, which I call *aggregation*, emerges from the combination of small bits of seemingly innocuous data.[84] When combined, the information becomes much more telling about a person. For the person who truly has nothing to hide, aggregation is not much of a problem. But in the stronger, less absolutist form of the nothing to hide argument, people argue that certain pieces of information are not something they would hide. Aggregation, however, means that by combining pieces of information we might not care to conceal, the government can glean information about us that we might really want to conceal. Part of the allure of data mining for the government is its ability to reveal a lot about our personalities and activities by sophisticated means of analyzing data. Therefore, without greater transparency in data mining, it is hard to claim that programs like the NSA data mining program will not reveal information people might want to hide, as we do not know precisely what is revealed. Moreover, data mining aims to be predictive of behavior, striving to prognosticate about our future actions. People who match certain profiles are deemed likely to engage in a similar pattern of behavior. It is quite difficult to refute actions that one has not yet done. Having nothing to hide will not always dispel predictions of future activity.

Another problem in the taxonomy, which is implicated by the NSA program, is the problem I refer to as *exclusion*.[85] Exclusion is the problem caused when people are prevented from having knowledge about how their information is being used, as well as barred from being

83. *Id.*
84. Solove, *supra* note 56, at 506–11.
85. *Id.* at 522–25.

able to access and correct errors in that data. The NSA program involves a massive database of information that individuals cannot access. Indeed, the very existence of the program was kept secret for years.[86] This kind of information processing, which forbids people's knowledge or 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. Moreover, it creates a power imbalance between individuals and the government. To what extent should the Executive Branch and an agency such as the NSA, which is relatively insulated from the political process and public accountability, have a significant power over citizens? This issue is not about whether the information gathered is something people want to hide, but rather about the power and the structure of government.

A related problem involves "secondary use." Secondary use is the use of data obtained for one purpose for a different unrelated purpose without the person's consent. The Administration has said little about how long the data will be stored, how it will be used, and what it could be used for in the future. The potential future uses of any piece of personal information are vast, and without limits or accountability on how that information is used, it is hard for people to assess the dangers of the data being in the government's control.

Therefore, 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—and not others. It assumes a particular view about what privacy entails, and it sets the terms for debate in a manner that is often unproductive.

It is important to distinguish here between two ways of justifying a program such as the NSA surveillance and data mining program. The first way is to not 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 NSA program outweigh the privacy harms. 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

86. Risen & Lichtblau, *supra* note 1.

things. But there are many other types of harm involved beyond exposing one's secrets to the government.

Privacy problems are often difficult to recognize and redress because they create a panoply of types of harm. Courts, legislators, and others look for particular types of harm to the exclusion of others, and their narrow focus blinds them to seeing other kinds of harms.

B. Understanding Structural Problems

One of the difficulties with the nothing to hide argument is that it looks for a visceral kind of injury as opposed to a structural one. Ironically, this underlying conception of injury is shared by both those advocating for greater privacy protections and those arguing in favor of the conflicting interests to privacy. For example, law professor Ann Bartow argues that I have failed to describe privacy harms in a compelling manner in my article, *A Taxonomy of Privacy*, where I provide a framework for understanding the manifold different privacy problems.[87] Bartow's primary complaint is that my taxonomy "frames privacy harms in dry, analytical terms that fail to sufficiently identify and animate the compelling ways that privacy violations can negatively impact the lives of living, breathing human beings beyond simply provoking feelings of unease."[88] Bartow claims that the taxonomy does not have "enough 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 categories of tort law."[89]

Most privacy problems lack dead bodies. Of course, there are exceptional cases such as the murders of Rebecca Shaeffer and Amy Boyer. Rebecca Shaeffer was an actress killed when a stalker obtained her address from a Department of Motor Vehicles record.[90] This incident prompted Congress to pass the Driver's Privacy Protection Act of 1994.[91] Amy Boyer was murdered by a stalker who obtained her personal information, including her work address and Social Security number, from a database company.[92] These examples aside, there is not a lot of death and gore in privacy law. If this is the standard to recognize a problem, then few privacy problems will be recognized. Horrific cases

87. Ann Bartow, *A Feeling of Unease About Privacy Law*, 155 U. PA. L. REV. PENNumbra 52, 52 (2006), http://www.pennumbra.com/issues/articles/154-3/Bartow.pdf.
88. *Id.*
89. *Id.* at 52, 62.
90. SOLOVE, *supra* note 4, at 147.
91. *Id.*
92. Remsburg v. Docusearch, Inc., 816 A.2d 1001, 1005–06 (N.H. 2003).

are not typical, and the purpose of my taxonomy is to explain why most privacy problems are still harmful despite this fact.

Bartow's objection is actually very similar to the nothing to hide argument. Those advancing the nothing to hide argument have in mind a particular kind of visceral privacy harm, one where privacy is violated only when something deeply embarrassing or discrediting is revealed. Bartow's quest for horror stories represents a similar desire to find visceral privacy harms. The problem is that not all privacy harms are like this. At the end of the day, privacy is not a horror movie, and demanding more palpable harms will be difficult in many cases. Yet there is still a harm worth addressing, even if it is not sensationalistic.

In many instances, privacy is threatened not by singular egregious acts, but by a slow series of relatively minor acts which gradually begin to add up. In this way, privacy problems resemble certain environmental harms which occur over time through a series of small acts by different actors. Bartow wants to point to a major spill, but gradual pollution by a multitude of different actors often creates worse problems.

The law frequently struggles with recognizing harms that do not result in embarrassment, humiliation, or physical or psychological injury.[93] For example, after the September 11 attacks, several airlines gave their passenger records to federal agencies in direct violation of their privacy policies. The federal agencies used the data to study airline security.[94] A group of passengers sued Northwest Airlines for disclosing their personal information. One of their claims was that Northwest Airlines breached its contract with the passengers. In *Dyer v. Northwest Airlines Corp*., the court rejected the contract claim because "broad statements of company policy do not generally give rise to contract claims," the passengers never claimed they relied upon the policy or even read it, and they "failed to allege any contractual damages arising out of the alleged breach."[95] Another court reached a similar conclusion.[96]

Regardless of the merits of the decisions on contract law, the cases represent a difficulty with the legal system in addressing privacy problems.

93. SOLOVE, *supra* note 4, at 93–97, 100–01, 195–208; Daniel J. Solove, *Identity Theft, Privacy, and the Architecture of Vulnerability*, 54 HASTINGS L.J. 1227, 1228 (2003).

94. SOLOVE, *supra* note 4, at 93.

95. 334 F. Supp. 2d 1196, 1200 (D.N.D. 2004).

96. *In re* Nw. Airlines Privacy Litig., No. 04-126, 2004 WL 1278459 (D. Minn. June 6, 2004).

The disclosure of the passenger records represented a "breach of confidentiality."[97] The problems caused by breaches of confidentiality do not merely consist of individual emotional distress; they involve a violation of trust within a relationship. There is a strong social value in ensuring that promises are kept and that trust is maintained in relationships between businesses and their customers. The problem of secondary use is also implicated in this case.[98] Secondary use involves data collected for one purpose being used for an unrelated purpose without people's consent. The airlines gave passenger information to the government for an entirely different purpose beyond that for which it was originally gathered. Secondary use problems often do not cause financial, or even psychological, injuries. Instead, the harm is one of power imbalance. In *Dyer*, data was disseminated in a way that ignored airline passengers' interests in the data despite promises made in the privacy policy. Even if the passengers were unaware of the policy, there is a social value in ensuring that companies adhere to established limits on the way they use personal information. Otherwise, any stated limits become meaningless, and companies have discretion to boundlessly use data. Such a state of affairs can leave nearly all consumers in a powerless position. The harm, then, is less one to particular individuals than it is a structural harm.

A similar problem surfaces in another case, *Smith v. Chase Manhattan Bank*.[99] A group of plaintiffs sued Chase Manhattan Bank for selling customer information to third parties in violation of its privacy policy, which stated that the information would remain confidential. The court held that even presuming these allegations were true, the plaintiffs could not prove any actual injury:

> [T]he "harm" at the heart of this purported class action, is that class members were merely offered products and services which they were free to decline. This does not qualify as actual harm.
>
> The complaint does not allege any single instance where a named plaintiff or any class member suffered any actual harm due to the receipt of an unwanted telephone solicitation or a piece of junk mail.[100]

The court's view of harm, however, did not account for the breach of confidentiality.

When balancing privacy against security, the privacy harms are often characterized in terms of injuries to the individual, and the interest in security is often characterized in a more broad societal way. The security

97. Solove, *supra* note 56, at 526–30.
98. *Id.* at 520–22.
99. 741 N.Y.S.2d 100 (N.Y. App. Div. 2002).
100. *Id.* at 102.

interest in the NSA programs has often been defined improperly. 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.[101]

The balance between privacy and security is often cast in terms of whether a particular government information collection activity should or should not be barred.

The issue, however, often is not whether the NSA or other government agencies should be allowed to engage in particular forms of information gathering; rather, it is what kinds of oversight and accountability we want in place when the government engages in searches and seizures. The government can employ nearly any kind of investigatory activity with a warrant supported by probable cause. This is a mechanism of oversight—it forces government officials to justify their suspicions to a neutral judge or magistrate before engaging in the tactic. For example, electronic surveillance law allows for wiretapping, but limits the practice with judicial supervision, procedures to minimize the breadth of the wiretapping, and requirements that the law enforcement officials report back to the court to prevent abuses.[102] It is these procedures that the Bush Administration has ignored by engaging in the warrantless NSA surveillance. The question is not whether we want the government to monitor such conversations, but whether the Executive Branch should adhere to the appropriate oversight procedures that Congress has enacted into law, or should covertly ignore any oversight.

Therefore, the security interest should not get weighed in its totality against the privacy interest. Rather, what should get weighed is the extent of marginal limitation on the effectiveness of a government information gathering or data mining program by imposing judicial oversight and minimization procedures. Only in cases where such procedures will completely impair the government program should the security interest

101. *Wartime Executive Power and the National Security Agency's Surveillance Authority: Hearing Before the S. Comm. on the Judiciary*, 109th Cong. 15 (2006) (statement of Alberto Gonzales, Att'y Gen. of the United States).

102. Daniel J. Solove, *Fourth Amendment Codification and Professor Kerr's Misguided Call for Judicial Deference*, 74 FORDHAM L. REV. 747, 775–76 (2005).

be weighed in total, rather than in the marginal difference between an unencumbered program versus a limited one.

Far too often, the balancing of privacy interests against security interests takes place in a manner that severely shortchanges the privacy interest while inflating the security interests. Such is the logic of the nothing to hide argument. When the argument is unpacked, and its underlying assumptions examined and challenged, we can see how it shifts the debate to its terms, in which it draws power from its unfair advantage. It is time to pull the curtain on the nothing to hide argument.

V. CONCLUSION

Whether explicit or not, conceptions of privacy underpin nearly every argument made about privacy, even the common quip "I've got nothing to hide." As I have sought to demonstrate in this essay, understanding privacy as a pluralistic conception reveals that we are often talking past each other when discussing privacy issues. By focusing more specifically on the related problems under the rubric of "privacy," we can better address each problem rather than ignore or conflate them. 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 in government surveillance and data mining programs. When engaged with 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.