2013

The Fight to Frame Privacy

Woodrow Hartzog
Boston University School of Law

THE FIGHT TO FRAME PRIVACY

*Woodrow Hartzog**

NOTHING TO HIDE: THE FALSE TRADEOFF BETWEEN PRIVACY AND SECURITY. By *Daniel J. Solove*. New Haven and London: Yale University Press. 2011. Pp. ix, 210. Cloth, $25; paper, $18.

INTRODUCTION

The resolution of a debate often hinges on how the problem being debated is presented. In communication, sociology, psychology, and related disciplines, this method of issue presentation is known as framing.[1] Framing theory holds that even small changes in the presentation of an issue or event can produce significant changes of opinion.[2] For example, people are more willing to tolerate rallies by controversial hate groups when such rallies are framed as free speech issues, rather than disruptions of the public order.[3]

Consider two questions: As guardians of civil rights, how should judges protect our privacy against the ever-increasing scope of government surveillance? When should judges defer to other branches of government that are better suited to understand when surveillance is necessary to ensure our national security? While these questions are constructed differently, disputes involving privacy and security can utilize either one. Yet the interchangeability of these questions should not be taken to mean that their construction is neutral. Indeed, the choice of which question to ask may predetermine the outcome of the dispute.

---

* Assistant Professor, Cumberland School of Law at Samford University; Affiliate Scholar, Center for Internet and Society at Stanford Law School. The author would like to thank Brannon Denning, Daniel Kreiss, Vance Ricks, Ryan Calo, Neil Richards, Danielle Citron, Cathy Packer, and Daniel Solove for their helpful comments.

1. *See, e.g.*, ERVING GOFFMAN, FRAME ANALYSIS (1974); Robert D. Benford & David A. Snow, *Framing Processes and Social Movements: An Overview and Assessment*, 26 ANN. REV. SOC. 611, 614 (2000); Dennis Chong & James N. Druckman, *Framing Theory*, 10 ANN. REV. POL. SCI. 103, 104 (2007); Laura E. Drake & William A. Donohue, *Communicative Framing Theory in Conflict Resolution*, 23 COMM. RES. 297, 300 (1996); Daniel Kahneman & Amos Tversky, *Choices, Values, and Frames*, 39 AM. PSYCHOLOGIST 341, 341 (1984); Deborah Tannen, *What's in a Frame? Surface Evidence for Underlying Expectations*, *in* FRAMING IN DISCOURSE 14, 15 (Deborah Tannen ed., 1993); Amos Tversky & Daniel Kahneman, *The Framing of Decisions and the Psychology of Choice*, 211 SCIENCE 453, 453 (1981).

2. *See, e.g.*, Thomas E. Nelson et al., *Toward a Psychology of Framing Effects*, 19 POL. BEHAV. 221, 224 (1997) ("Frames can be meaningful and important determinants of public opinion.").

3. Thomas E. Nelson et al., *Media Framing of a Civil Liberties Conflict and Its Effect on Tolerance*, 91 AM. POL. SCI. REV. 567 (1997). Another author provides this example: "[A]n 80 percent chance to survive a medical operation may mean something different to a consumer than a 20 percent chance to die on the operating table, even though these two 'frames' convey mathematically equivalent information." Richard L. Hasen, *Efficiency Under Informational Asymmetry: The Effect of Framing on Legal Rules*, 38 UCLA L. REV. 391, 393 (1990).

Judges, lawmakers, and the public all use and are influenced by frames.[4] This influence is particularly important in the battle for privacy and security. To date, the dominant frame pits security against privacy. Those who support government collection and analysis of personal information in the name of security often justify any accompanying threats to privacy with some form of the argument, "I've got nothing to hide." This statement implies that privacy is only needed if a person is concealing wrongdoing. By this account, privacy must yield to security measures because privacy appears less justified than security.[5]

In his important new book, *Nothing to Hide: The False Tradeoff Between Privacy and Security*, Daniel Solove[6] argues that if we continue to view privacy and security as diametrically opposed to each other, privacy will always lose. Solove argues that the predetermined abandonment of privacy in security-related disputes means that the structure of the privacy–security debate is inherently flawed. Solove understands that privacy is far too vital to our freedom and democracy to accept its inevitable demise.

The central thesis of this Review is that Solove's polemic is a strong and desperately needed collection of frames that counterbalances the "nothing to hide" argument and other refrains so often used in privacy disputes. *Nothing to Hide* is succinct and accessible. In his ambitious quest to concisely respond to a wide range of problems, however, Solove risks leaving the reader unsatisfied, wanting more details about his proposals to untangle the tension between privacy and security.[7] Yet this critique does not detract from the

4. *See, e.g.*, Judith D. Fischer, *Got Issues? An Empirical Study About Framing Them*, 6 J. Ass'n Legal Writing Directors 1, 3 (2009) ("Researchers have applied framing theory to show that frames affect how people see issues. This analysis has helped politicians influence public opinion by skillfully framing ideas. Similarly, a skillfully framed issue statement can help shape a court's perceptions of an appellate case." (footnotes omitted)); Chris Guthrie, *Prospect Theory, Risk Preference, and the Law*, 97 Nw. U. L. Rev. 1115, 1128 (2003) ("[F]raming can negatively influence judicial intervention in settlement talks."); Jonathan Remy Nash & Stephanie M. Stern, *Property Frames*, 87 Wash. U. L. Rev. 449 (2010); Cass R. Sunstein, *Moral Heuristics and Moral Framing*, 88 Minn. L. Rev. 1556, 1559 (2004); Daniel M. Isaacs, Note, *Baseline Framing in Sentencing*, 121 Yale L.J. 426 (2011).

5. *See, e.g.*, Richard A. Posner, *Privacy, Surveillance, and Law*, 75 U. Chi. L. Rev. 245, 251 (2008) ("Privacy is the terrorist's best friend . . . ."); Richard A. Posner, *The Right of Privacy*, 12 Ga. L. Rev. 393, 398 (1978) ("At some point nondisclosure becomes fraud."); *see also* Stewart A. Baker, Skating on Stilts: Why We Aren't Stopping Tomorrow's Terrorism (2010); Amitai Etzioni, The Limits of Privacy (1999).

6. John Marshall Harlan Research Professor of Law, The George Washington University Law School.

7. Solove concedes this point, explaining that his focus is on general arguments and principles instead of technical minutiae. P. vii ("Of course, the details are important, but even more important are the basic concepts and themes of this debate."). For a more technical treatment of some of the issues in the book, Solove recommends his previous scholarly work on the topic. *See* Daniel J. Solove, *Data Mining and the Security-Liberty Debate*, 75 U. Chi. L. Rev. 343 (2008); Daniel J. Solove, *The First Amendment as Criminal Procedure*, 82 N.Y.U. L. Rev. 112 (2007); Daniel J. Solove, *Fourth Amendment Codification and Professor Kerr's Misguided Call for Judicial Deference*, 74 Fordham L. Rev. 747 (2005); Daniel J. Solove, *Fourth Amendment Pragmatism*, 51 B.C. L. Rev. 1511 (2010); Daniel J. Solove, *"I've Got Nothing to Hide" and Other Misunderstandings of Privacy*, 44 San Diego L. Rev. 745

importance of this book as a collection of frames to counter a popular narrative in the privacy and security debate.

Part I of this Review discusses the central arguments of the book by examining frames that are contrary to the commonly adopted narratives. Instead of reviewing the numerous arguments in the order in which they appear in the book, this Review consolidates the arguments into groups of frames, such as the "judges as guardians" frame, the "privacy as a societal value" frame, and the "fruitless focus" frame.

Part II addresses some of the "security side" arguments that deserve more attention, including the framing of proposed security measures as feasible or works in progress that must be deployed in order to be improved on. Part III proposes several additional frames that support the basic premise of *Nothing to Hide*, including confidentiality, obscurity, and the commonalities between privacy and security.

I. Nothing to Hide

Nothing to Hide attempts to address four main concerns and is organized accordingly in four parts: (1) how lawmakers and the public should assess and balance the values of privacy and security; (2) how the law should address matters of national security; (3) how the Constitution should protect privacy; and (4) how the law should cope with changing technology. The book is designed so that one can read the chapters independently of one another.

This book has been published at a time when the debate regarding privacy and security seems more prominent than ever. Multiple privacy-related statutes have been proposed in Congress,[8] and Congress has held multiple hearings on the state of privacy.[9] The media have devoted substantial attention

(2007); Daniel J. Solove, *Melville's* Billy Budd *and Security in Times of Crisis*, 26 Cardozo L. Rev. 2443 (2005); Daniel J. Solove, *Reconstructing Electronic Surveillance Law*, 72 Geo. Wash. L. Rev. 1264 (2004).

8. *See e.g.*, Electronic Communications Privacy Act Modernization Act of 2012, H.R. 6339, 112th Cong. (2012) (proposed by Rep. Nadler and Rep. Conyers); Protect America's Privacy Act of 2012, S. 3515, 112th Cong. (2012) (proposed by Sen. Merkley); Electronic Communications Privacy Act Amendments Act of 2011, S. 1011, 112th Cong. (2011) (proposed by Sen. Leahy); Do-Not-Track Online Act of 2011, S. 913, 112th Cong. (2011) (proposed by Sen. Rockefeller); Commercial Privacy Bill of Rights Act of 2011, S. 799, 112th Cong. (2011) (proposed by Sen. Kerry and Sen. McCain); *see also EPIC Bill Track Tracking Privacy, Speech, and Cyber-Liberties Bills in the 111th Congress*, Electronic Privacy Information Center, http://epic.org/privacy/bill_track.html (last visited Oct. 22, 2012).

9. *See, e.g.*, *What Facial Recognition Technology Means for Privacy and Civil Liberties: Hearing Before the Subcomm. on Privacy, Tech. & the Law of the S. Comm. on the Judiciary*, 112th Cong. (2012); *Protecting Mobile Privacy: Your Smartphones, Tablets, Cell Phones and Your Privacy: Hearing Before the Subcomm. on Privacy, Tech. & the Law of the S. Comm. on the Judiciary*, 112th Cong. (2012); *The Electronic Communications Privacy Act: Government Perspectives on Protecting Privacy in the Digital Age: Hearing Before the S. Comm. on the Judiciary*, 112th Cong. (2011); *The State of Online Consumer Privacy: Hearing Before the S. Comm. on Commerce, Science, & Transp.*, 112th Cong. (2011).

to the importance and erosion of privacy in the information age.[10] A number of high–profile privacy violations—including invasive body scanners at airports, the massive scope of government surveillance of internet and phone communications, and large-scale data breaches involving personal information—have impacted enormous segments of the American public.[11] How people frame all of these issues affects how the issues are debated.

A. *A Brief Exploration of Framing*

Framing offers a way to articulate the "power of a communicating text."[12] According to Robert Entman, "To frame is to select some aspects of a perceived reality and make them more salient in a communicating text, in such a way as to promote a particular problem definition, causal interpretation, moral evaluation, and/or treatment recommendation for the item described."[13] By increasing the salience of certain bits of information, frames enhance the probability that receivers will perceive the information in a certain way, discern a particular meaning, and process it accordingly.[14]

While frames do not guarantee an influence on audience thinking, frames that comport with the existing schemata in a receiver's belief system can be particularly effective.[15] Daniel Kahneman and Amos Tversky offered what is now likely the most well-known example of how framing works by highlighting some features while omitting others.[16] In an experiment, the researchers asked test subjects the following hypothetical:

---

10. *See, e.g.*, Steve Lohr, *How Privacy Vanishes Online*, N.Y. Times, Mar. 16, 2010, at A1, http://www.nytimes.com/2010/03/17/technology/17privacy.html; Jeffrey Rosen, *The Web Means the End of Forgetting*, N.Y. Times, July 21, 2010, at MM30, http://www.nytimes.com/2010/07/25/magazine/25privacy-t2.html; *What They Know*, Wall St. J., http://online.wsj.com/public/page/what-they-know-digital-privacy.html (last visited Oct. 23, 2012).

11. *See, e.g.*, Eric Lichtblau, *Wireless Firms Are Flooded by Requests to Aid Surveillance*, N.Y. Times, July 8, 2012, at A1, http://www.nytimes.com/2012/07/09/us/cell-carriers-see-uptick-in-requests-to-aid-surveillance.html; James Bamford, *The NSA Is Building the Country's Biggest Spy Center (Watch What You Say)*, Wired (Mar. 15, 2012, 7:24 PM), http://www.wired.com/threatlevel/2012/03/ff_nsadatacenter/all/1; Sean Gallagher, *Data Breaches Increasingly Caused by Hacks, Malicious Attacks*, Ars Technica (Mar. 20, 2012, 1:33 PM), http://arstechnica.com/business/2012/03/data-breaches-increasingly-caused-by-hacks-malicious-attacks/; *Whole Body Imaging Technology and Body Scanners ("Backscatter" X-Ray and Millimeter Wave Screening)*, Electronic Privacy Info. Center, http://epic.org/privacy/airtravel/backscatter/ (last visited Oct. 7, 2012); *Chronology of Data Breaches: Security Breaches 2005-Present*, Privacy Rights Clearinghouse, http://www.privacyrights.org/data-breach (last updated Oct. 21, 2012).

12. Robert M. Entman, *Framing: Toward Clarification of a Fractured Paradigm*, J. Comm., Autumn 1993, at 51, 51.

13. *Id.* at 52 (italics omitted).

14. *Id.* at 53.

15. *Id.* at 53–54 ("The notion of framing thus implies that the frame has a common effect on large portions of the receiving audience, though it is not likely to have a universal effect on all.").

16. Kahneman & Tversky, *supra* note 1.

> Imagine that the U.S. is preparing for the outbreak of an unusual Asian disease, which is expected to kill 600 people. Two alternative programs to combat the disease have been proposed. Assume that the exact scientific estimates of the programs are as follows:
>
> If Program A is adopted, 200 people will be saved. . . .
>
> If Program B is adopted, there is a one-third probability that 600 people will be saved and a two-thirds probability that no people will be saved. . . .
>
> Which of the two programs would you favor?[17]

Here, 72% chose Program A.[18] Kahneman and Tversky followed this experiment with another that offered mathematically *identical options* for treating the same situation, but the programs were framed in terms of *likely deaths* rather than *lives saved*:

> If Program C is adopted, 400 people will die . . . .
>
> If Program D is adopted, there is a one-third probability that nobody will die and a two-thirds probability that 600 people will die.[19]

With this alternative framing, 22% chose Program C, even though 72% of the previous experimental group selected Program A, Program C's mathematical twin.[20] In short, the alternative framing resulted in a reversal of the percentages.

In discussing this famous experiment, Entman stated, "As this example vividly illustrates, the frame determines whether most people notice and how they understand and remember a problem, as well as how they evaluate and choose to act upon it."[21] Perhaps one of the most important functions of frames is that by calling attention to particular aspects of a described reality, they, by construction, direct attention away from other facets.[22] According to Entman, this logical sleight of hand means that "[m]ost frames are defined by what they omit as well as include, and the omissions of potential problem definitions, explanations, evaluations, and recommendations may be as critical as the inclusions in guiding the audience."[23]

---

17. *Id.* at 343.

18. *Id.*

19. *Id.*

20. *Id.* Conversely, 78 percent of respondents chose Program D even though previously 28 percent chose Program D's clone, Program B. Kahneman and Tversky gave members of both experimental groups only two treatment options from which to choose. *Id.*

21. Entman, *supra* note 12, at 54.

22. *Id.*

23. *Id.*; *see also* Murray Edelman, *Contestable Categories and Public Opinion,* 10 POL. COMM. 231, 232 (1993) ("The character, causes, and consequences of any phenomenon become radically different as changes are made in what is prominently displayed, what is repressed and especially in how observations are classified . . . . [T]he social world is . . . a kaleidoscope of potential realities, any of which can be readily evoked by altering the ways in which observations are framed and categorized.").

The omissions of the current framing of the privacy and security debate are what motivate *Nothing to Hide* (p. 24). Framing the debate in terms of security versus privacy ignores many alternative aspects of the reality of the debate. Courts, legislators, scholars, attorneys, and the media fixate on questions of *whether* privacy should be protected, at the expense of novel approaches as to *how* privacy should be protected (p. 3). The more this narrative continues, the more entrenched it becomes. Thus, the framing of a debate is not an insignificant matter.[24] The choice of words and construction of frames can have significant consequences for legal disputes and, consequently, our civil rights.[25] Some frames, such as the "nothing to hide" argument, can take hold in certain contexts and can be very difficult to shake or balance (pp. 21–32). This is why alternatives to the current narrative, like those that Solove offers, are so important in the fight to frame privacy.

B. Nothing to Hide*'s Framing of Privacy*

Solove's body of work displays a keen understanding of how the privacy–security debate deeply influences government collection and use of personal information. *Nothing to Hide* centers on a major problem of the debate, which is that privacy too often needlessly loses out to security (p. 2). One reason for this is that security is articulated as the need to protect "life and limb," while the notion of privacy rights is more amorphous. Solove finds that under the common narrative, people believe that they must sacrifice privacy in order to be more secure (pp. 21–24, 33). And advocates of certain security measures make powerful arguments to encourage others to accept this trade-off (p. 2).

This is where framing theory comes into play. Solove notes that people have incorrectly framed the debate between privacy and security, portraying the trade-off between these values as an all-or-nothing proposition (p. 2). *Nothing to Hide* is based on the idea that the protection of privacy need not be fatal to security measures; it merely demands oversight and regulation. Solove asserts that the debate between privacy and security cannot progress because the structure of the debate itself is fundamentally flawed (p. 2).

Solove demonstrates that he understands the importance of frames when he states, "The way problems are conceived has a tremendous impact on the legal and policy solutions used to solve them" (p. 24). Solove draws on his philosophical guide, John Dewey, who observed, "A problem well put is

---

24. *See, e.g.*, Robert D. Benford & David A. Snow, *Framing Processes and Social Movements: An Overview and Assessment*, 26 ANN. REV. SOC. 611 (2000); Sarah Kaplan, *Framing Contests: Strategy Making Under Uncertainty*, 19 ORG. SCI. 729 (2008); Deana A. Rohlinger, *Framing the Abortion Debate: Organizational Resources, Media Strategies, and Movement-Countermovement Dynamics*, 43 SOC. Q. 479 (2002).

25. *See* PAUL M. SNIDERMAN ET AL., REASONING AND CHOICE 52 (1991) ("The effect of framing is to prime values differently, establishing the salience of one or the other . . . . [Thus] a majority of the public supports the rights of persons with AIDS when the issue is framed [in a survey question] to accentuate civil liberties considerations—and supports . . . mandatory testing when the issue is framed to accentuate public health considerations.").

half-solved" (p. 24; footnote omitted). To that end, Solove offers numerous arguments, which can be seen as "frames," that balance the privacy–security debate by focusing on how privacy should be protected, rather than if it should be protected (pp. 24–26).

Solove develops five dominant frames in the book. He conceptualizes privacy as a plurality of different things instead of simply "secrecy." He frames many of the arguments espoused by security-side advocates as false dichotomies. He characterizes judges as guardians and warns against excessive and misguided deference to governmental entities in the privacy–security debate. He describes much of the focus on whether privacy should be protected as fruitless. Finally, Solove highlights that privacy is not just an individual value but also a societal one, and he accentuates the many benefits of privacy.

1. Privacy as a Plurality of Different Things Versus Antiquated Notions of Privacy

One of Solove's principal goals in *Nothing to Hide* is to highlight the fact that many of the dominant frames that are used in privacy and security issues rely on antiquated conceptualizations of privacy. The first antiquated notion of privacy is at the very core of the book: "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' " (p. 21). Solove claims that the "nothing to hide" argument is a fallacy because it relies on the faulty assumption that privacy is about just hiding bad things (pp. 26–29).

Privacy protects against more than just the harm that could result from disclosing secrets. Additionally, privacy is not often threatened by a single egregious act or lost in one fell swoop. Instead, Solove asserts that privacy is "often eroded over time, little bits dissolving almost imperceptibly until we finally begin to notice how much is gone" (p. 30). This "incremental harm" frame can be used to counter the "nothing to hide" argument with respect to government surveillance (p. 30). Incremental increases in surveillance ultimately allow the government to collect massive dossiers of our "activities, interests, reading habits, finances, and health" (p. 31).

No area of privacy law seems to rely on antiquated notions of privacy more than the Fourth Amendment. According to Solove, the antiquated notion that drives Fourth Amendment jurisprudence is that "something is private only if it is completely secret" (p. 94). This "secrecy paradigm" is out of touch with modern society because it dictates that if you share your information with other people or entities, including internet service providers ("ISPs"), websites, or even trusted friends, you cannot expect privacy (p. 100). Taken to its logical conclusion, the secrecy paradigm forces a choice between living the life of a hermit or relinquishing our privacy and, in turn, a key protection against excessive government surveillance.[26] Solove rightly notes that this approach is unsustainable in a world where online activity, which necessarily involves disclosing information to others, is increasingly a mandatory aspect of participating in society (p. 110).

The secrecy paradigm owes part of its entrenchment to another antiquity of Fourth Amendment law known as the "third-party doctrine." This doctrine typically holds that "if [personal] information is in the hands of a third party, then [a person has] no reasonable expectation of privacy in it—and as a result, no Fourth Amendment protection" (p. 102). Solove unequivocally argues that "the third party doctrine is one of the greatest threats to privacy in our times" (p. 103).

The problems with the third-party doctrine in defining privacy as secrecy become more evident with each newly adopted technology (Chapter Eleven). ISP records and cloud computing are unprotected by the Fourth Amendment (pp. 105–06). As a result, Solove argues, "[a] company can't meaningfully promise you confidentiality, because the government won't respect that promise" (p. 107). Solove accurately pinpoints one of the main problems with the third-party doctrine—its failure to account for the concepts of confidentiality, promises, and contracts (pp. 108–09). As is discussed in Part III, Solove could have explored these concepts further as a response to the current problems with Fourth Amendment doctrine.

Confidentiality, promises, and contracts, which are not only critical to businesses and commerce but are also important in our social lives, are entrenched in the law. So why are they irrelevant in determining privacy expectations under the Fourth Amendment? The answer is that Fourth Amendment doctrine generally requires a person disclosing information to assume the risk of harm that might come from disclosure (p. 108). Those subscribing to the "nothing to hide" argument might not have a problem with assuming the risk. After all, if a person has nothing to hide, then government surveillance poses no threat.

Consider, however, social media such as Facebook. If Facebook users are simply gossiping with their friends and posting pictures for hundreds to see, should they be able to claim any privacy interest in information that the government wants for security purposes? Given that these users are still vulnerable to privacy-related harms, the answer must be yes. Issues of data protection, transparency, limits on use, and aggregation are no less vital simply because the medium is "social." All online information is shared

---

26. One of Solove's most satisfying criticisms is a response to the argument that if you want privacy, you should "just keep your data to yourself":

> So don't use a credit card. Don't have cable. Don't use the Internet. Don't use the phone. Don't have a bank account. Don't have insurance. Don't go to a hospital. Don't have a job. Don't rent an apartment. Don't subscribe to any magazines or newspapers. Don't do anything that creates a record.
>
> In other words, go live as a hermit in a cabin on a mountaintop. That's where the Fourth Amendment still protects you.

P. 110.

with someone, if only the user's ISP and the recipient website. By reframing privacy as a plurality of different values rather than simply secrecy, the debate no longer hinges on whether a person has completely concealed the information. Rather, people can have a more nuanced discussion about the many different privacy interests implicated by the government's collection and use of information. Additionally, judges and lawmakers who embrace a pluralistic conception of privacy can then consider varying degrees of protection, from thin to robust.

2. False Dichotomies

One problem with the current all-or-nothing frames used in the privacy and security debate is that they are false dichotomies. According to Solove, the common refrain is that we can have privacy *or* security, but in many instances, we can't have both (pp. 33–37). Solove contends that this argument is flawed because sacrificing privacy does not necessarily make us more secure. Indeed, many security measures do not invade privacy, and there is no direct relationship between the effectiveness of a security measure and the amount of liberty (p. 34). As I argue in Part III, Solove also could have argued that in many instances, such as certain settings involving encryption, security protections can actually ensure privacy.

According to Solove, the problem with balancing privacy against security is that too often people assume that an entire security measure is in the balance, even though protecting privacy seldom negates a security measure altogether (p. 37). Recall that framing is effective not only because it makes some aspects of a dispute salient but also because it hides some logical aspects as a result.[27] Here, the all-or-nothing frame obscures the option for judicial oversight of a security measure to ensure due process that would only incrementally burden security while protecting privacy. The only way to accurately evaluate the costs of protecting privacy is to reject the all-or-nothing frame.

Unfortunately, the false dichotomies in the privacy and security debate are unlikely to dissipate anytime soon. Consider the increasing use of unmanned aircraft, often called drones, for surveillance, which will likely be the next battlefield for privacy and security.[28] Privacy advocates have objected to the use of drones for relentless and pervasive surveillance of the American public.[29] Framed as an all-or-nothing debate, advocates of drone

---

27. *See supra* note 16 and accompanying text.

28. *See, e.g.*, M. Ryan Calo, *The Drone as Privacy Catalyst*, 64 Stan. L. Rev. Online 29, 30 (2011) ("[Drones] threaten to perfect the art of surveillance. Drones are capable of finding or following a specific person. They can fly patterns in search of suspicious activities or hover over a location in wait . . . . In addition to high-resolution cameras and microphones, drones can be equipped with thermal imaging and the capacity to intercept wireless communications.").

29. *See, e.g.*, Jennifer Lynch, *Are Drones Watching You?*, Electronic Frontier Foundation (Jan. 10, 2012), https://www.eff.org/deeplinks/2012/01/drones-are-watching-you.

surveillance might argue that it would be harmful to outlaw drones just because they might cause privacy problems. Drones simply have too much potential to dramatically improve the efficiency of law enforcement. Privacy advocates might respond by seeking to keep drones out of the skies. Both responses would be too extreme.

Solove's false-dichotomy frame accentuates a possible middle ground. The government could effectively use drones while still respecting privacy by limiting the duration of observation, the focus subject, and the amount of information collected or retained, and by subjecting the use of drones to the process of judicial oversight. The government could engage in long-term or general searches, seen as anathema in Fourth Amendment doctrine,[30] on a limited basis and only in extreme circumstances, such as riots and mass attacks on the public, and with obligations to incorporate certain data protections, such as restricted data retention rules.[31]

3. Misguided Deference (and Judges as Guardians)

Because the "nothing to hide" frame concerns the appropriateness of an intelligence-gathering measure, it deftly obscures the antecedent question in the privacy and security debate, which is whether the measure is even effective. To help address the question of efficacy, Solove asks why judges give so much deference to executive decisions. Solove states, "Deference is a major problem when it comes to balancing security and privacy. Although courts should not take a know-it-all attitude, they shouldn't defer on such a critical question as a security measure's effectiveness" (pp. 39–40). Instead, Solove proposes that courts and lawmakers require justifications from experts for the security measures that they advocate (p. 41). After all, the point of judicial review is to scrutinize the actions of government officials, not to accept their authority without question.

Solove draws on one of the most compelling and established descriptions of the judiciary to support his claim of misguided deference, which is that judges are guardians of an individual's privacy and civil liberties (pp. 41–42). As such, they are well equipped to ensure the balance between security and liberty. Although this balance might not allow the maximization of security, Solove poignantly observes that accepting less than complete security "is one of the costs of living in a democracy as opposed to an authoritarian political regime."[32]

While it might seem that Solove views the courts as the most appropriate architects of privacy and security law, this is not the case. In the

30. *E.g.*, Lloyd L. Weinreb, *Generalities of the Fourth Amendment*, 42 U. CHI. L. REV. 47, 50 (1974) ("The central theme of the [Fourth] [A]mendment is its prohibition against general searches, the evil that its authors had foremost in mind.").

31. I thank Ryan Calo for this insightful point.

32. P. 41. Solove goes on to assert that the judiciary gives too much deference to the executive branch in exercising its war powers, pp. 42–46, and gives too much deference to legislators, who have muddled privacy law in many areas such as electronic surveillance. Pp. 165–66.

misguided-deference frame, Solove continues his crusade against the all-or-nothing tenor of the privacy and security debate by tasking the courts with both rigor and deference. The branches of government, he suggests, should challenge each other and compromise when possible when confronted with a problematic security measure. Solove's vision is not that judges create their own ideal security measures but rather that they evaluate the security measures of the executive and legislative branches to force them to justify their policies (pp. 40–41).

4. Fruitless Focus

Much of *Nothing to Hide* is dedicated to the proposition that privacy-protection regimes are often such a mess because they focus on the wrong issues. This misguided focus can lead to perverse or absurd results. Ironically, one of Solove's core arguments is that "the Fourth Amendment would better protect privacy if the Supreme Court stopped focusing on it" (p. 113). More specifically, Solove proposes abandoning the "reasonable expectation of privacy" test, which has vexed nearly everyone since its inception (pp. 114–15): "Instead, we should focus on the practical consequences of Fourth Amendment coverage . . . . [W]henever a particular government information-gathering activity creates problems of reasonable significance, the Fourth Amendment should require regulation and oversight" (pp. 115–16). By increasing the salience of the energy wasted in trying to determine whether information is private, and thus subject to protection, the fruitless-focus frame advances the discussion by assuming a broad Fourth Amendment applicability; it asks how an information-gathering activity or security measure should be regulated so as to balance privacy protections with security protections.[33]

5. Privacy's Values and Goals

One of the most problematic aspects of the "nothing to hide" argument is that it buries privacy's underlying and associated values by focusing on the need for security. Solove remedies this by framing privacy as a core First Amendment concept and a tool to effectuate due process and equality. For example, Solove argues that while the Fourth Amendment regulates how the government can gather information about individuals, the collection and use of such information can also affect an individual's First Amendment rights, including the freedoms of speech, association, thought, and belief (p. 146).

The knowledge that the government is gathering information about an individual could inhibit that individual from exercising her First Amendment

33. Another example of the fruitless-focus frame involves the hastily enacted USA PATRIOT Act. Many view this statute as the law that destroyed privacy in America. Solove, however, argues that "all the hoopla has been focused too much on the Patriot Act itself and not enough on the law more generally. Many of the complaints about the Patriot Act relate to problems with the law that existed long before the act was ever passed." P. 156. Instead, Solove argues that electronic-surveillance law must be entirely reworked. P. 156.

rights. This reluctance of expression is commonly known as a "chilling effect," and scholars have recognized it as something that the First Amendment seeks to protect against.[34] Solove argues that since the First and Fourth Amendments share a common history, and the Fourth Amendment no longer adequately protects against government information gathering that threatens to chill speech, association, and intellectual inquiry, "the First Amendment should be considered alongside the Fourth Amendment as a source of criminal procedure" (pp. 146–52).

Given the prominence of the First Amendment in policy debates, this frame could be extremely powerful. Recall that people are more willing to tolerate rallies by controversial hate groups when such rallies are framed as free speech issues rather than disruptions of the public order.[35] Later in the book, Solove notes the threat that government data mining—that is, amassing personal data about individuals to create profiles for later use by the government—poses to First Amendment–protected activities (pp. 189–90). Solove observes that information gathering might inhibit protected activities, such as reading, socializing, and even merely using internet search engines (p. 189).

Perhaps the most important frame that Solove offers with respect to underlying values is the conceptualization of privacy as a societal, not individual, right. According to Solove, since the current frame balances the safety of society versus the privacy of an individual, the security interest almost always wins (p. 47). Solove argues that a society without privacy protection would be oppressive and that, accordingly, we must consider the social value of privacy as a civil liberty (Chapter Five).

6. Other Frames

One of the most effective frames employed by Solove is "security theater," (p. 44) a term that security expert Bruce Schneier popularized.[36] According to Schneier, "Security theater refers to security measures that make people feel more secure without doing anything to actually improve their security."[37] Schneier gives as an example the practice of checking for

34. *See, e.g.*, Frederick Schauer, *Fear, Risk and the First Amendment: Unraveling the "Chilling Effect"*, 58 B.U. L. Rev. 685, 688 (1978) ("[T]he chilling effect doctrine recognizes the fact that the legal system is imperfect and mandates the formulation of legal rules that reflect our preference for errors made in favor of free speech."). Neil Richards has argued that individuals need what he has described as "intellectual privacy" in order to protect our intellectual freedom to think without state oversight or interference. *See* Neil Richards, *The Dangers of Surveillance*, 126 Harv. L. Rev. (forthcoming 2013), *available at* http://www.harvardlawreview.org/symposium/papers2012/richards.pdf ("Surveillance is harmful because it can chill the exercise of our civil liberties, and because it gives the watcher power over the watched . . . . Such intellectual surveillance is particularly dangerous because it can cause people not to experiment with new, controversial, or deviant ideas.").

35. Nelson et al., *supra* note 3, at 574.

36. *See* Bruce Schneier, *Beyond Security Theater*, Schneier on Security (Nov. 13, 2009, 6:52 AM), http://www.schneier.com/blog/archives/2009/11/beyond_security.html.

37. *Id.*

photo IDs in office buildings. He states, "No-one has ever explained why verifying that someone has a photo ID provides any actual security, but it looks like security to have a uniformed guard-for-hire looking at ID cards."[38] Solove gives as an additional example the New York City subway search program, whereby armed guards randomly searched a relatively small number of subway passengers. According to Solove, this security measure was largely symbolic because it involved only a miniscule fraction of the subway's daily passengers, and a potential terrorist could have easily avoided the searches by simply getting off at a different station (p. 39).

Of course, security theater has some utility—it can lower public anxiety over security threats because the security measure is highly visible. But Solove rejects security theater, stating, "Meaningful protection of rights requires that they be sacrificed only when security measures are really effective. Rights shouldn't be sacrificed for lies, no matter how noble the intention behind the lies might be."[39] Solove's critique of security theater seems appropriate, given some of the problematic approaches to security today. Many Americans have objected to the increasingly invasive and dubious nature of airport security as well as the money spent on questionable security technologies, such as the more than $30 million spent on "puffer" machines, which remain in storage because they are unreliable.[40] Security theater could also be part of the justification for ubiquitous public surveillance cameras, which, as Solove explains in Chapter 18, are not very effective in lowering crime. Apparently even the theatrical aspects of the cameras are a failure, as Solove notes that the numerous public cameras deployed in the United Kingdom have failed to reduce people's fear of crime (p. 180).

The final part of *Nothing to Hide* is dedicated to how the law should cope with changing technology. This section also develops new frames to counter the current structure of the debate surrounding privacy and changing technology. For example, where advocates of new security technologies, such as biometrics, would call the opponents of these measures Luddites, Solove would describe the opponents as rightfully cautious (pp. 199–205). Where advocates of ubiquitous video surveillance argue that you should not expect any privacy in public, Solove frames the issue as one of effectiveness. He

---

38. *Id.*

39. P. 45. Solove memorably states, "If we give up some privacy for security, we should at least get our money's worth, not placebos or empty symbolic measures." P. 45.

40. *See, e.g.*, Thomas Frank, *It's the Last Gasp for Bomb-Sensing 'Puffers' at Airports*, USA TODAY, May 21, 2009, http://usatoday30.usatoday.com/travel/flights/2009-05-20-puffers_N.htm?csp; Kip Hawley, *Why Airport Security Is Broken—And How to Fix It*, WALL ST. J., Apr. 15, 2012, http://online.wsj.com/article/SB10001424052702303815404577335783535660546.html ("The relationship between the public and the TSA has become too poisonous to be sustained."); *Confrontation with TSA Agent Leaves Grandpa's Ashes on Floor*, THE INDY CHANNEL (June 25, 2012), http://www.theindychannel.com/news/31224633/detail.html (quoting a man whose grandfather's ashes were spilled at a TSA security checkpoint, "I want an apology from TSA. I want an apology from the lady who opened the jar and laughed at me. I want them to help me understand where they get off treating people like this").

wonders who will watch the watchers and cites evidence that surveillance cameras only seem to shift crime to areas that the cameras do not cover (pp. 180–81).

The frames that Solove offers are essential to help balance the privacy and security debate. The government can appropriately and proportionately implement security measures only when such measures are not framed as false dichotomies or by antiquated notions of privacy. In this way, security measures can become more efficient and less invasive of privacy. However, *Nothing to Hide* does not offer a complete solution to the problems inherent in the privacy and security debate. The book consciously sacrifices technical minutiae and explicit details to focus on general arguments and principles (p. vii). This trade-off makes *Nothing to Hide* one of the most accessible books on the privacy and security debate. But empirical support and explicit details are eventually necessary to fully embrace Solove's arguments.

II. Security-Side Frames

Although *Nothing to Hide* does an excellent job critiquing the current structure of the privacy and security debate, a few of the "security side" frames deserve further exploration. Many proponents of security measures frame the major issue of the debate as one of simplicity and feasibility. Because *Nothing to Hide* offers general remedies instead of highly detailed solutions, Solove's arguments are vulnerable to one of the most common attacks on many proposals to protect privacy—blurring the bright line. For concepts such as the third-party doctrine, the current distinction between protected and unprotected information is clear and largely ascertainable. Advocates of the third-party doctrine, such as Orin Kerr, extol its clarity and feasibility in justifying its place in Fourth Amendment jurisprudence.[41]

When framed as an issue of practicality, concepts like the third-party doctrine might seem more attractive than some of Solove's proposals, which might be difficult for law enforcement officials to follow because they are either generalized or highly context-dependent. For example, Solove's pragmatic approach for examining the legitimacy of a security measure includes vague questions such as "Does it work well?" and "Does it cause any problems for privacy and civil liberties?" (p. 208). Solove also argues that the Fourth Amendment should dictate that searches are unreasonable in all situations in which the government gathers personal information and that information-gathering activity creates a problem that is not addressed with some form of regulation or oversight (p. 122).

But these proposals require additional guidance to be effectively implemented. When exactly does a security measure work well? When the measure has a high success rate or a low error rate? Is Solove contemplating normative or legal privacy problems as part of his pragmatic approach? Must the problems contemplated by Solove rise to the level of a clear legal

41. *See* Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 Mich. L. Rev. 561, 581–83 (2009).

violation or just a cognizable harm? Lawmakers, courts, and other relevant stakeholders are certainly capable of answering these questions. Fourth Amendment doctrine and other bodies of law have refined and articulated their boundaries and nuances over time, and Solove's pragmatic approach could evolve the same way. But until it does, supporters of the status quo might view Solove's proposal as a threat to bright-line rules such as the third-party doctrine, which, for all its problems, is relatively easy to implement in practice.

Another security-side frame that deserves additional attention is the conceptualization of security measures as an ongoing process. Much of Solove's critique of privacy-invasive security measures is that they are ineffective (pp. 38–46). One counter to this argument could be to concede the initial ineffectiveness of security measures and argue that the only way such measures will improve is through trial, error, and innovation. If governments do not have some flexibility in the implementation and improvement of a security measure, that inflexibility might foreclose the possibility of a more effective, and perhaps less privacy-invasive, security measure.

For example, later in the book, Solove tackles the problems of predictive data mining—that is, the use of data in personal profiles to make predictive determinations about one's future behavior. Solove gives as an example denying someone the ability to travel due to a predictive judgment based on previously collected data that the person is a security threat (pp. 196–97). Even selecting someone for extra scrutiny could be a form of predictive data mining, a technique that Solove argues comes with more costs than benefits (p. 196).

Solove's problem with predictive data mining is that it destroys too much privacy for such a speculative return. He assails the technique's extremely small likelihood of success, stating, "Finding a terrorist among the millions who travel each day is like finding a needle in a haystack. An individual fitting a profile may be statistically likelier to be a terrorist than someone who doesn't fit it, but the chances are still very small." (p. 197). This is an efficacy and cost–benefit argument, which leaves open the counterargument that more accurate data mining could justify invasions of privacy. If so, proponents of data mining might argue that the government must be given the flexibility to refine its algorithms to make the trade-off of privacy more reasonable.

For example, what would the data-mining debate look like if a particular technique could accurately identify a threat 99 percent of the time with a false negative rate of less than 1 percent?[42] Even if such a low failure rate were possible, rigorous trial and error in "real-world" settings would likely be required for this kind of accuracy. Thus, Solove wisely incorporates principles of autonomy, antidiscrimination, freedom of expression, and other

42. A false negative is "[a] negative test result when the attribute for which the subject is being tested actually exists in that subject." THE AMERICAN HERITAGE STEDMAN'S MEDICAL DICTIONARY 292 (2d ed. 2004).

civil liberties into his critique of data mining to balance the "necessary flexibility" frame that is enabled by a cost–benefit analysis.[43]

III. Additional Frames

Nothing to Hide is an excellent touchstone on which to begin reframing the privacy and security debate. However, other frames not fully explored in the book could also advance Solove's general thesis, including the similarities between privacy and security, a more pronounced focus on confidentiality, and the importance of the concept of obscurity in our everyday lives. Solove has well explored some of these concepts, such as confidentiality, in other works, while those in the privacy and security debate have not yet fully embraced other concepts, such as obscurity.

A. *The Commonalities Between Privacy and Security*

Solove could support his narrative that privacy and security are not opposing forces by detailing their similarities. Instead of focusing on security as "national security" or "crime prevention," which predominate the book, Solove could focus on how people secure their own information from others. In this way, he could make the commonalities between privacy and security salient and, thus, less adversarial in the broader debate.

Security and privacy often coexist. In many instances, the security of personal information actually guarantees its privacy, even if privacy was merely an ancillary benefit resulting from a security measure. Consider encryption technologies, which allow users to keep a communication secure by concealing the contents of a message or transmission.[44] Encryption programs such as Pretty Good Privacy allow users to protect the privacy of their personal information by ensuring that only authorized users can access the information; in other words, users protect their private information by securing it.[45]

---

43. Solove addresses but does not fully explore these themes:

> People shouldn't be systematically treated worse than other people for factors they have no power to change . . . . [A traveler] shouldn't have to refrain from doing things he's legally entitled to do [based on his behavior profile]. He shouldn't have to answer to government officials for who he is or what he does. Otherwise, he's being treated no longer as an equal but as someone who is inherently suspicious. No law-abiding citizen should be treated this way.

P. 197.

44. For two books that provide detailed histories of the advancement of encryption technology, see Steven Levy, Crypto: How the Code Rebels Beat the Government—Saving Privacy in the Digital Age (2001), and Simon Singh, The Code Book (1999).

45. Margaret Rouse, *Pretty Good Privacy (PGP)*, SearchSecurity, http://searchsecurity.techtarget.com/definition/Pretty-Good-Privacy (last updated Sept. 2005); *cf.* Derek E. Bambauer, *Privacy Versus Security*, J. Crim. L. & Criminology (forthcoming 2013 (manuscript at 4)), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2208824 (citing literature that recognizes "that privacy and security (as implemented through cryptography) are different, though complimentary").

Of course, this security means that information important for national security purposes might be unavailable to the government. The U.S. government has argued that it needs access to encryption keys for this very reason.[46] Here, encryption can also allow users to protect information that needs in order to remain secret to prevent crime or for national security purposes. Indeed, encryption is regularly employed by the government and other third parties to protect classified information.[47] Thus, one could frame the argument that encryption should be weakened within the broader concept of "security," not just obtaining incriminating information from guilty parties. In these instances, asking individuals to give up their privacy can be tantamount to compromising security, which makes the request to sacrifice privacy for a different kind of security seem perverse.

B. *Confidentiality*

Solove is one of the most prolific modern thinkers on confidentiality law.[48] While he mentions the importance of confidentiality in *Nothing to Hide*, he leaves the concept's potential as a frame in the privacy and security debate largely untapped, particularly as an alternative to the third-party doctrine. Solove states, "The third party doctrine fails to comprehend the concept of confidentiality—as well as the concept of a promise" (p. 108).

Solove observes that although nongovernmental actors generally respect promises of confidentiality, the third-party doctrine ensures that even a written contract is not sufficient to give people an expectation of privacy (p. 108). Solove then poignantly notes, "But promises and contracts are the foundation of modern civil society. If people couldn't rely on them, business and commerce would grind to a halt. Yet when it comes to privacy, the U.S. Supreme Court thinks that promises and contracts don't matter."[49] At this point, Solove's exploration of confidentiality gives way to other faults with the third-party doctrine.

46. *E.g.*, A. Michael Froomkin, *The Metaphor Is the Key: Cryptography, the Clipper Chip, and the Constitution*, 143 U. PA. L. REV. 709 (1995) (exploring the "Clipper Chip," a federal encryption standard in which the government would retain a copy of the encryption key in an escrow).

47. *E.g.*, *NSA Suite B Cryptography*, NAT'L SECURITY AGENCY, http://www.nsa.gov/ia/programs/suiteb_cryptography/ (last updated Sept. 24, 2012); *see, e.g.*, *EAR Controls for Items that Use Encryption*, U.S. BUREAU OF INDUSTRY & SECURITY, http://www.bis.doc.gov/encryption/ (last visited July 9, 2012).

48. *See, e.g.*, Neil M. Richards & Daniel J. Solove, *Privacy's Other Path: Recovering the Law of Confidentiality*, 96 GEO. L.J. 123 (2007) [hereinafter Richards & Solove, *Privacy's Other Path*]; Neil M. Richards & Daniel J. Solove, *Prosser's Privacy Law: A Mixed Legacy*, 98 CALIF. L. REV. 1887 (2010); Daniel J. Solove & Neil M. Richards, *Rethinking Free Speech and Civil Liability*, 109 COLUM. L. REV. 1650 (2009).

49. Pp. 108–09. Solove also points out the hypocrisy of the government's promising to protect the confidentiality of census answers in light of the third-party doctrine, stating, "The government respects its own promises of confidentiality, yet it runs roughshod over everybody else's." P. 107.

But confidentiality law could play a larger role in this debate, as an alternative to the third-party doctrine and as part of Solove's general proposal that the Fourth Amendment should apply whenever government information gathering causes privacy problems.[50] Confidentiality law is quite old and well developed.[51] Indeed, it predates the American conceptualization of privacy law.[52] Not only does this entrenched concept make courts' reliance on the third-party doctrine seem absurd by contrast, but confidentiality also sits at the ready as an ample body of law from which one can determine whether information is deserving of protections.

C. *Obscurity*

The "nothing to hide" argument and the "no privacy in public" argument completely disregard one of the most important concepts in our social lives—obscurity.[53] This concept, which has been strangely ignored or undeveloped by courts, lawmakers, scholars, and other policy stakeholders, supports Solove's argument that privacy is about more than hiding and secrecy. Obscurity—which in its simplest form is a state of being unknown by others, though not necessarily completely hidden—helps explain why most individuals would balk at having their every public activity continually monitored even if they might not expect their activities in public to be a complete secret.[54] Obscurity generally refers to the lack of knowledge or understanding of a person or piece of information.[55]

> An individual is obscure to an observer if the observer does not possess or comprehend critical information needed to make sense of the individual. Personal identity, social connections, and personal or situational context are examples of such critical information. Without this information, the observer has a limited ability to make sense of the actions and utterances of the individual.[56]

Obscurity explains why we are comfortable talking about personal information in a crowded restaurant and posting personal information to a

---

50. *See* pp. 121–22, 208.

51. Richards & Solove, *Privacy's Other Path*, *supra* note 48.

52. *Id.* at 133.

53. Portions of this section have been adapted from the author's previous posts at the website for the Center for Internet and Society at Stanford Law School and www.usvjones.com. *See, e.g.*, Woodrow Hartzog, *Three Cheers for Obscurity, an Unspoken Beneficiary of* United States v. Jones, The Center for Internet & Soc'y (Feb. 2, 2012, 9:59 AM), http://cyberlaw.stanford.edu/blog/2012/02/three-cheers-obscurity-unspoken-beneficiary-united-states-v-jones; Woodrow Hartzog, United States v. Jones *and the Need to Embrace Obscurity*, USvJones.com, http://usvjones.com/2012/06/02/united-states-v-jones-and-the-need-to-embrace-obscurity/#more-156 (last visited Oct. 5, 2012).

54. Woodrow Hartzog & Frederic Stutzman, *The Case for Online Obscurity*, 101 Calif. L. Rev. (forthcoming 2013) (manuscript at 4–8), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1597745.

55. *Id.* at 4.

56. *Id.* at 5.

restricted number of people within online communities. Indeed, a significant portion of our everyday interaction places us into a zone of obscurity, where our identity and personal context are unknown to those we interact with or with whom we share common space.[57] Socialization typically depends on some ability to manage the accessibility and comprehension of social exchanges by outsiders, the loss of which can be quite harmful.[58]

The recent Supreme Court decision in *United States v. Jones* illustrates the need for the obscurity frame in privacy doctrine.[59] On its face, *Jones* stands for the proposition that the government's installation of a GPS device on a target's vehicle, and its use of that device to monitor the vehicle's movements, constitutes a Fourth Amendment search.[60] The decision was unanimous on this narrow point, though the concurring opinions by Justices Sotomayor and Alito are more remarkable than the majority opinion because they question the conventional wisdom surrounding the use of ubiquitous surveillance technologies.[61] Because the majority opinion focused on the attachment of the device to the car, it avoided tackling the much more difficult issue of whether individuals can have privacy in "public." Perhaps the obscurity frame can advance the dialogue on this issue.

Neither the majority opinion nor the concurring opinions in *Jones* explicitly reference the concept of obscurity. Justices Sotomayor and Alito, however, seem to indicate in their concurring opinions a willingness to protect obscure personal information.[62] An embrace of obscurity would be significant because the concept can alleviate the inflexibility of the third-party doctrine and, more importantly, loosen the public–private dichotomy's grip on Fourth Amendment jurisprudence.

But justices are unlikely to embrace obscurity overnight. After the *Katz v. United States* decision,[63] Fourth Amendment decisions have centered on whether individuals had a "reasonable expectation of privacy" (pp. 98–99,

---

57. *Id.* Consider how many unidentified people interact with each other in restaurants, office buildings, public transportation, and the like.

58. IRWIN ALTMAN, THE ENVIRONMENT AND SOCIAL BEHAVIOR (1975); ERVING GOFFMAN, THE PRESENTATION OF SELF IN EVERYDAY LIFE (1959); ERVING GOFFMAN, BEHAVIOR IN PUBLIC PLACES: NOTES ON THE SOCIAL ORGANIZATION OF GATHERINGS (1966); SANDRA PETRONIO, BOUNDARIES OF PRIVACY: DIALECTICS OF DISCOURSE (2002); Erving Goffman, *Felicity's Condition*, 89 AM. J. SOC. 1, 51 (1983); Geoffrey A. Fowler, *When the Most Personal Secrets Get Outed on Facebook*, WALL ST. J., Oct. 13, 2012, at A1, http://online.wsj.com/article/SB10000872396390444165804578008740578200224.html (describing the harmful effects of inadvertently disclosing information known only to a small group on the social network site Facebook).

59. *See* 132 S. Ct. 945, 955 (2012) (Sotomayor, J., concurring); *id*. at 963–64.

60. *Jones*, 132 S. Ct. at 949 (majority opinion); *id.* at 954 (Sotomayor, J., concurring).

61. *See id.* at 957 (Sotomayor J., concurring); *id*. at 964 (Alito, J., concurring in the judgment).

62. *See id.* at 954–57 (Sotomayor, J., concurring); *id.* at 963–64.

63. Katz v. United States, 389 U.S. 347, 353 (1967) (concluding that "The Government's activities in electronically listening to and recording the petitioner's words violated the privacy upon which he justifiably relied while using the telephone booth and thus constituted a 'search and seizure' within the meaning of the Fourth Amendment.").

Chapter Twelve). Yet it is obscurity that lies at the heart of many critical Fourth Amendment disputes. For example, the desire for privacy in public can be accurately reframed as a preference for or expectation of obscurity. Critiques that the third-party doctrine and the "secrecy paradigm" are too harsh reflect an implicit preference for the protection of information that is shared with some but not all.[64]

In *Jones*, Justice Sotomayor proposed that it might be time to abandon the third-party doctrine precisely because she was not ready to accept that the limited disclosure of information to others automatically abrogated an individual's Fourth Amendment rights.[65] Sotomayor's position is, in essence, a recognition of maintaining the hidden nature of some kinds of information, which, while known by some, is likely to remain obscure to most.[66]

Appreciation for obscurity can also be found in the so-called "mosaic theory" of the Fourth Amendment, which has been articulated as the approach "by which courts evaluate a collective sequence of government activity as an aggregated whole to consider whether the sequence amounts to a search."[67] In the aggregate, our day-to-day activities create a revealing picture of our entire lives.[68] Yet, when they are considered in isolation, these pieces of information are less likely to reveal sensitive details of one's life. These discrete pieces of information are often fully understood by only a few, known to some, accessible to many others, and obscure to the general public. Individuals have an interest in ensuring that this information is hard to find and understand. The difficulty of discovery and comprehension provides for obscurity, which is destroyed when this information is ubiquitously collected and aggregated.[69]

---

64. Daniel J. Solove, The Digital Person 42 (2004).

65. *Jones*, 132 S. Ct. at 957 (2012) (Sotomayor, J., concurring) ("[I]t may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties.").

66. *See id.*

67. Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 Mich. L. Rev. 311, 313 (2012) ("Identifying Fourth Amendment searches requires analyzing police actions over time as a collective 'mosaic' of surveillance; the mosaic can count as a collective Fourth Amendment search even though the individual steps taken in isolation do not.").

68. *Jones*, 132 S. Ct. at 955 (Sotomayor, J., concurring) ("GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations.").

69. For instance, in *United States v. Maynard*, Judge Ginsburg stated the following:

> The whole of one's movements over the course of a month is not constructively exposed to the public because, like a rap sheet, that whole reveals far more than the individual movements it comprises. The difference is not one of degree but of kind, for no single journey reveals the habits and patterns that mark the distinction between a day in the life and a way of life, nor the departure from a routine that, like the dog that did not bark in the Sherlock Holmes story, may reveal even more.
>
> As with the "mosaic theory" often invoked by the Government in cases involving national security information, "What may seem trivial to the uninformed, may appear of great moment to one who has a broad view of the scene."

615 F.3d 544, 561–62 (D.C. Cir. 2010) (citations omitted), *aff'd in part*, *Jones*, 132 S.Ct. 945.

Justice Sotomayor's concurring opinion in *Jones* can be seen as receptive to the concept of obscurity. In *Jones,* she stated that she would take into account the ubiquity of GPS monitoring when considering whether an individual had a reasonable societal expectation of privacy in the entirety of an individual's public movements.[70] Specifically, Justice Sotomayor stated that she "would ask whether people reasonably expect that their movements will be recorded and aggregated in a manner that enables the Government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on."[71]

Justice Alito's concurring opinion also implicitly valued obscurity by focusing on the length of monitoring, rather than the majority's focus on trespass, to find a Fourth Amendment search.[72] Alito noted that individuals value and rely on the difficulty of finding personal information.[73]

The privacy value inherent in the practical difficulties of collecting and understanding information has previously been recognized by the Supreme Court in *U.S. Department of Justice v. Reporters Committee for Freedom of the Press*.[74] In that case, the Court recognized the privacy interest in maintaining the "practical obscurity" of geographically dispersed public records that were later aggregated into comprehensive "rap sheets."[75]

In *Jones,* Justice Alito noted that society has traditionally expected that others, including law enforcement agents, would refrain from continuous, long-term surveillance, if for no other reason than that such monitoring would be cost prohibitive.[76] Following this rationale, individuals expect and need most of the details of their lives to remain ephemeral. Long-term continuous surveillance reverses society's expectations by ensuring that most of the details of an individual's life are collected during the surveillance period. In other words, long-term, continuous surveillance results in the loss of an individual's obscurity.

Like privacy, obscurity is an expansive concept. But one can refine it for use in various contexts. For example, in previous research, my coauthor and

---

70. *Jones*, 132 S. Ct. at 956 (Sotomayor, J., concurring).

71. *Id.*

72. *Id.* at 958 (Alito, J., concurring in the judgment).

73. *Id.* at 963 ("In the pre-computer age, the greatest protections of privacy were neither constitutional nor statutory, but practical. Traditional surveillance for any extended period of time was difficult and costly and therefore rarely undertaken.").

74. 489 U.S. 749, 770 (1989).

75. *Reporters Comm.*, 489 U.S. at 780 ("The privacy interest in maintaining the practical obscurity of rap-sheet information will always be high. When the subject of such a rap sheet is a private citizen and when the information is in the Government's control as a compilation, rather than as a record of 'what the Government is up to,' the privacy interest protected by [the personal privacy exemption to the Freedom of Information Act] is in fact at its apex . . . .").

76. *Jones*, 132 S. Ct. at 964 (Alito, J., concurring in the judgment) ("[S]ociety's expectation has been that law enforcement agents and others would not—and indeed, in the main, simply could not—secretly monitor and catalogue every single movement of an individual's car for a very long period.").

I have conceptualized online obscurity as information that "exists in a context missing one or more key factors that are essential to discovery or comprehension."[77] We proposed that there were four factors to online obscurity: (1) search visibility, (2) unprotected access, (3) identification, and (4) clarity.[78] Fourth Amendment doctrine could look to the degree of obscurity of online information instead of asking whether it was public or private.

Framing privacy as obscurity would help resolve the issue of privacy in online information that has been disclosed to others. Information that is often perceived as "public," such as information disclosed to a select few via the social web, can still be obscure. If courts looked to the obscurity of information, a determination of whether the information was "publicly available" would only be one part of a more nuanced inquiry. An offline conceptualization of obscurity might vary from its online counterpart, perhaps by adhering closer to the Supreme Court's conceptualization of "practical obscurity" in *Reporters Committee*.[79] Regardless, it is becoming increasingly difficult for courts and lawmakers to justify ignoring a concept that is vital to social interaction.

The inquiry as to whether individuals can have privacy in public often feels intractable. Courts and lawmakers have strained to articulate a valid privacy interest in information that others could theoretically access yet are unlikely to find or understand. A refined concept of obscurity could be utilized as a frame to respond to the "nothing to hide" argument by demonstrating that most aspects of a person's life are, to some degree, hidden and as a consequence, relatively protected.

Conclusion

The "nothing to hide" frame employed in the privacy and security debate has for far too long demanded the wrong kind of justification from critics of a government's security measures. When the question is effectively framed as "How long have you wanted to protect criminals?," critics are asked to submit to a false dichotomy between staying safe or protecting lawbreakers. Daniel Solove's *Nothing to Hide: The False Tradeoff Between Privacy and Security* will help change the structure of this debate.

This important book offers many new ways to frame the approach to privacy and security, which will help restore balance to this important policy conversation. By framing secrecy as an antiquated notion of privacy, judges as guardians of our civil liberties, privacy as a societal value, and poor oversight of security measures as an issue of misguided deference, Solove provides a roadmap for those who seek to respond to arguments such as "I've got nothing to hide."

Solove's critique of the way the privacy and security debate has been framed is empowering. A focus on framing enables additional critiques be-

77. Hartzog & Stutzman, *supra* note 54.

78. *Id.*

79. *Reporters Comm.*, 489 U.S. at 780.

yond what is included in *Nothing to Hide*. Some examples of additional critiques include the commonalities of privacy and security, the disclosure of information as an issue of confidentiality, and public surveillance as a threat to our cherished obscurity, rather than a threat to some vague and often untenable expectation of privacy. One can see the utility of Solove's frames and the additional frames proposed in this Review in many current privacy and security disputes involving social media, drones, and GPS technologies, including the recent Supreme Court opinion *United States v. Jones*.

Nothing to Hide is concise and direct. Although it lacks the technical minutiae and empirics found in many law and policy books, it is destined to become an important work for those who seek to understand how privacy and security relate to each other in our modern world. In rejecting the preordained conclusion that privacy must give way to security, Solove reframes the structure of the debate as one aimed at maximizing security while providing the proper oversight and limits on government surveillance. These restrictions are necessary to protect our privacy, a concept that has always been about more than just hiding.