2015

The Self, the Stasi, the NSA: Privacy, Knowledge, and Complicity in the Surveillance State

Richard Warner
IIT Chicago-Kent College of Law, rwarner@kentlaw.iit.edu

Robert H. Sloan
University of Illinois at Chicago, sloan@uic.edu

The Self, the Stasi, the NSA: Privacy, Knowledge, and Complicity in the Surveillance State

Robert H. Sloan* **and Richard Warner****

ABSTRACT

We focus on privacy in public. The notion dates back over a century, at least to the work of the German sociologist, Georg Simmel. Simmel observed that people voluntarily limit their knowledge of each other as they interact in a wide variety of social and commercial roles, thereby making certain information private relative to the interaction even if it is otherwise publicly available. Current governmental surveillance in the US (and elsewhere) reduces privacy in public. But to what extent?

The question matters because adequate self-realization requires adequate privacy in public. That in turn depends on informational norms, social norms that govern the collection, use, and distribution of information. Adherence to such norms is constitutive of a variety of relationships in which parties coordinate their use of information. Examples include student/teacher and journalist/confidential source. Current surveillance undermines privacy in public by undermining norm-enabled coordination. The 1950 to 1990 East German

---

* Professor and Head, Department of Computer Science, University of Illinois at Chicago.

** Professor of Law, Chicago-Kent College of Law, Visiting Foreign Professor, University of Gdansk, Poland.

We presented earlier drafts at the 2014 Midwest Privacy Scholars Conference at Notre Dame, and at a Faculty Workshop at the Chicago-Kent College of Law. We thank the participants for their insightful and encouraging comments. We are also indebted to Lori Andrews for her perceptive comments that showed the way to a proper organization of the material. We owe thanks to Christopher Buccafusco for comments that sharpened our discussion of the dangers contained in current governmental surveillance.

Stasi illustrates the threat to self-realization. The "hidden, but for every citizen tangible omni-presence of the Stasi, damaged the very basic conditions for individual and societal creativity and development: Sense of one's self, Trust, Spontaneity."[1] *The United States is not East Germany, but it is on the road that leads there. And that raises the question of how far down that road it has traveled.*

To support the "on the road" claim and answer the "how far" question, we turn to game-theoretic studies of the Assurance Game (more popularly known as the Stag Hunt). We combine our analysis of that game with a characterization of current governmental surveillance in terms of five concepts: knowledge, use, merely knowing, complicity, and uncertainty. All five combine to undermine norm-enabled coordination. The Assurance Game shows how use—both legitimate and not legitimate—leads to discoordination. Enough discoordination would lead to a Stasi-like world. But will that happen? A comparison with the Stasi shows cause for concern. The United States possesses a degree of knowledge about its citizens that the Stasi could only dream of. Moreover—perhaps—it arguably surpasses the Stasi in complicity, even though Stasi informants "spied on friends, workmates, neighbours and family members. Husbands spied on wives."[2] *The Stasi only clearly exceeded the United States in repressive use. While it is difficult to predict the future of surveillance, we conclude with three probable scenarios. In only one is there an adequate degree of privacy in public.*

1. GARY BRUCE, THE FIRM: THE INSIDE STORY OF THE STASI 12 (2010) (quoting Hubertus Knabe as printed in SANDRA PINGEL-SCHLIEMANN, ZERSETZEN: STRATEGIE EINER DIKTATUR 50 (2002)).

2. LUKE HARDING, THE SNOWDEN FILES: THE INSIDE STORY OF THE WORLD'S MOST WANTED MAN 250 (2014).

INTRODUCTION

In 2007, the security expert Bruce Schneier noted,

> History will record what we, here in the early decades of the information age, did to foster freedom, liberty, and democracy. Did we build information technologies that protected people's freedoms even during times when society tried to subvert them? Or did we build technologies that could easily be modified to watch and control?[3]

Is the answer already obvious? A large literature now details the "watch and control" practices of businesses and governments.[4] Add Edward Snowden's revelations,[5] and it is

3. Bruce Schneier, *Risks of Data Reuse*, SCHNEIER ON SECURITY (June 28, 2007, 8:34 AM), https://www.schneier.com/blog/archives/2007/06/risks_of_data_r.html.

4. *See, e.g.*, JULIA ANGWIN, DRAGNET NATION: A QUEST FOR PRIVACY, SECURITY, AND FREEDOM IN A WORLD OF RELENTLESS SURVEILLANCE (2014); JAMES BAMFORD, THE SHADOW FACTORY: THE ULTRA-SECRET NSA FROM 9/11 TO THE EAVESDROPPING ON AMERICA (2008); HEIDI BOGHOSIAN, SPYING ON DEMOCRACY: GOVERNMENT SURVEILLANCE, CORPORATE POWER, AND PUBLIC RESISTANCE (2013); SIMON CHESTERMAN, ONE NATION UNDER SURVEILLANCE: A NEW SOCIAL CONTRACT TO DEFEND FREEDOM WITHOUT SACRIFICING LIBERTY (2011); RONALD J. DEIBERT, BLACK CODE: INSIDE THE

hard to avoid Schneier's own 2013 "watch and control" conclusion:

> So we're done. Welcome to a world where Google knows exactly what sort of porn you all like, and more about your interests than your spouse does. Welcome to a world where your cell phone company knows exactly where you are all the time. Welcome to the end of private conversations, because increasingly your conversations are conducted by e-mail, text, or social networking sites. And welcome to a world where all of this, and everything else that you do or is done on a computer, is saved, correlated, studied, passed around from company to company without your knowledge or consent; and where the government accesses it at will without a warrant. Welcome to an Internet without privacy, and we've ended up here with hardly a fight.[6]

Are we done? Our answer is, "Not yet." An adequate degree of privacy may still be possible. We conclude with a suggestion about what is necessary to make that possibility a reality.

We focus exclusively on governmental surveillance.[7] We also confine our attention to *informational* privacy, the ability

---

BATTLE FOR CYBERSPACE (2013); BEATRICE EDWARDS, THE RISE OF THE AMERICAN CORPORATE SECURITY STATE: SIX REASONS TO BE AFRAID (2014); LUIS A. FERNANDEZ, POLICING DISSENT: SOCIAL CONTROL AND THE ANTI-GLOBALIZATION MOVEMENT (2008); JOHN GILLIOM & TORIN MONAHAN, SUPERVISION: AN INTRODUCTION TO THE SURVEILLANCE SOCIETY (2013); GLENN GREENWALD, NO PLACE TO HIDE: EDWARD SNOWDEN, THE NSA, AND THE U. S. SURVEILLANCE STATE (2014); HARDING, *supra* note 2; SUSAN LANDAU, SURVEILLANCE OR SECURITY?: THE RISKS POSED BY NEW WIRETAPPING TECHNOLOGIES (2010); ROBERT H. SLOAN & RICHARD WARNER, UNAUTHORIZED ACCESS: THE CRISIS IN ONLINE PRIVACY AND SECURITY (2013) [hereinafter SLOAN & WARNER, UNAUTHORIZED ACCESS]; THE WASH. POST, NSA SECRETS: GOVERNMENT SPYING IN THE INTERNET AGE (2013); ATHAN G. THEOHARIS, ABUSE OF POWER: HOW COLD WAR SURVEILLANCE AND SECRECY POLICY SHAPED THE RESPONSE TO 9/11 (2011); Jon D. Michaels, *All the President's Spies: Private-Public Intelligence Partnerships in the War on Terror*, 96 CALIF. L. REV. 901 (2008); Joel R. Reidenberg, *The Data Surveillance State in the United States and Europe*, 49 WAKE FOREST L. REV. 583 (2014); Neil M. Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934 (2013).

5. *See e.g.*, GREENWALD, *supra* note 4; HARDING, *supra* note 2; THE WASH. POST, *supra* note 4.

6. Bruce Schneier, *The Internet Is a Surveillance State*, CNN (Mar. 16, 2013, 2:04 PM), http://www.cnn.com/2013/03/16/opinion/schneier-internet-surveillance/index.html [hereinafter *The Internet Is a Surveillance State*]. The warrant issues are far more complicated than Schneier suggests. *See generally* Christopher Slobogin, *Subpoenas and Privacy*, 54 DEPAUL L. REV. 805 (2005).

7. Private sector surveillance raises related concerns, as we have discussed elsewhere. *See* SLOAN & WARNER, UNAUTHORIZED ACCESS, *supra* note 4; Robert H. Sloan & Richard Warner, *Beyond Notice and Choice: Privacy, Norms, and Consent*, 14 SUFFOLK U. J. HIGH TECH. L. 370 (2014)

to determine what others do with your information.[8] Advances in information processing technology reduce privacy by giving others immense and increasing control over your information.[9] This is particularly true of privacy *in public*.[10] The notion of privacy in public dates back over a century, at least to the work

---

[hereinafter Sloan & Warner, *Beyond Notice*]; Robert H. Sloan & Richard Warner, *Big Data and the "New" Privacy Tradeoff*, *in* BIG DATA AND PRIVACY: MAKING ENDS MEET 110 (Future of Privacy Forum & Stanford Law Sch. Ctr. for Internet & Soc'y eds., 2013), http://www.futureofprivacy.org/big-data-privacy-workshop-paper-collection; Richard Warner & Robert H. Sloan, *Behavioral Advertising: From One-Sided Chicken to Informational Norms*, 15 VAND. J. ENT. & TECH. L. 49 (2012) [hereinafter Warner & Sloan, *Behavioral Advertising*]; Richard Warner & Robert H. Sloan, *Self, Privacy, and Power: Is It All Over?*, 17 TUL. J. TECH. INTELL. PROP. 61 (2014) [hereinafter Warner & Sloan, *Self, Privacy, and Power*].

8. ALAN F. WESTIN, PRIVACY AND FREEDOM 7 (1967); *see also* U.S. Dep't of Justice v. Reporters Comm. for Freedom of the Press, 489 U.S. 749, 763 (1989) ("[B]oth the common law and the literal understandings of privacy encompass the individual's control of information concerning his or her person."); JAMES B. RULE, PRIVACY IN PERIL 3 (2007) (defining privacy "as the exercise of an authentic option to withhold information on one's self"); Michael Froomkin, *The Death of Privacy*, 52 STAN. L. REV. 1461, 1463 (2000) ("I will use 'informational privacy' as shorthand for the ability to control the acquisition or release of information about oneself.").

9. *See, e.g.*, The Center for Digital Democracy & U.S. PIRG, Comment Letter on Preliminary FTC Staff Report on Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework For Businesses and Policymakers 1, 15–20 (Feb. 8, 2011), https://www.ftc.gov/sites/default/files/documents/public_comments/preliminary-ftc-staff-report-protecting-consumer-privacy-era-rapid-change-proposed-framework/00338-57839.pdf.

10. Helen Nissenbaum's work sparked the current focus on privacy in public. *See* Helen Nissenbaum, *Privacy as Contextual Integrity*, 79 WASH. L. REV. 119 (2004) [hereinafter Nissenbaum, *Privacy as Contextual*]; Helen Nissenbaum, *Protecting Privacy in an Information Age: The Problem of Privacy in Public*, 17 LAW & PHIL. 559 (1998) [hereinafter Nissenbaum, *Protecting Privacy*]; Helen Nissenbaum, *Toward an Approach to Privacy in Public: Challenges of Information Technology*, 7 ETHICS & BEHAV. 207 (1997). Our approach in terms of norms is indebted to her work. For other recognitions of privacy in public, see James W. Patton, *Protecting Privacy in Public? Surveillance Technologies and the Value of Public Places*, 2 ETHICS & INFO. TECH. 181 (2000); Herman T. Tavini, *Search Engines, Personal Information and the Problem of Privacy in Public*, 3 INT'L REV. INFO. ETHICS 39 (2005); Nick Taylor, *State Surveillance and the Right to Privacy*, 1 SURVEILLANCE & SOC'Y 66 (2002). A 2013 report from Canada's Information and Privacy Commissioner emphasizes the importance of privacy in public. ANN CAVOUKIAN, SURVEILLANCE, THEN AND NOW: SECURING PRIVACY IN PUBLIC SPACES (2013), http://www.ipc.on.ca/images/Resources/pbd-surveillance.pdf. There is a well-established practice in sociology of regarding privacy as existing in public through selective disclosure. *See, e.g.*, CHRISTENA NIPPERT-ENG, ISLANDS OF PRIVACY (2010).

of the German sociologist Georg Simmel, who observed that people voluntarily limit their knowledge of each other as they interact in a wide variety of social and commercial roles.[11] The mutual restraint ensures that information remains private *relative to the interaction* even if it is otherwise publicly available.[12]

Current governmental surveillance reduces privacy in public.[13] But to what extent? The question matters because adequate self-realization requires adequate privacy in public.[14] That in turn depends on informational norms, social norms that govern the collection, use, and distribution of information.[15] Current surveillance practices threaten to undermine norm-enabled coordination and thereby to undermine privacy in public. The 1950 to 1990 East German Stasi illustrates the threat. The "hidden, but for every citizen tangible omni-presence of the Stasi, damaged the very basic conditions for individual and societal creativity and development: Sense of one's self, Trust, Spontaneity."[16] The United States is not East Germany, but it is on the road that leads there. And that raises the question of how far it will travel. Sections I–IV support the "on the road" claim. Section V explores how far the United States will go down that road.

Section I characterizes the concept of privacy in public and argues that informational norms play a central role in the creating of privacy in public. Section II connects the loss of privacy in public to the loss of self-realization. Section III presents five surveillance concepts essential to our explanation of why governmental surveillance undermines norm-enabled privacy in public. Section IV uses that conceptual framework to

---

11. Georg Simmel, *The Sociology of Secrecy and of Secret Societies*, 11 AM. J. SOC. 441, 467–68 (1906).

12. The connection between privacy and the self is a standard theme in the privacy literature. *See, e.g.*, DANIEL J. SOLOVE, UNDERSTANDING PRIVACY 98 (2008) ("[T]heorists have proclaimed the value of privacy to be protecting intimacy, friendship, dignity, individuality, human relationships, autonomy, freedom, self-development, creativity, independence, imagination, counterculture, eccentricity, freedom of thought, democracy, reputation, and psychological well-being.").

13. *See* Nissenbaum, *Protecting Privacy*, *supra* note 10, at 561–63.

14. *See* Jeffrey H. Reiman, *Privacy, Intimacy, and Personhood*, 6 PHIL. & PUB. AFF. 26, 37 (1976) ("I shall myself argue that the right to privacy is fundamentally connected to personhood.").

15. Sloan & Warner, *Beyond Notice*, *supra* note 7, at 407–14.

16. BRUCE, *supra* note 1.

construct a model of how surveillance undermines privacy in public. Section V uses that model to address the question of how far the United States may travel down the road toward a Stasi-like world.

I. PRIVACY IN PUBLIC

A good way to introduce privacy in public is to begin with the question, Why isn't it a contradiction? After all, "purely 'private' things are completely inaccessible to others," while "[p]urely 'public' [things] are completely accessible to others."[17] Distinguishing different kinds of opposites dispels the appearance of contradiction.

Some opposites are completely mutually exclusive. Thus Lou Manheim to Bud Fox in *Wall Street*: "You can't be just a little bit pregnant when you are talking bankruptcy. You can't be just a little bit bankrupt. You are either bankrupt or not bankrupt."[18] There is no middle ground for "bankrupt/not bankrupt" and "pregnant/not pregnant." They are mutually exclusive. But not all opposites are. [19] Take cheap and expensive. Something can be a little cheap, or little expensive. "Cheap as possible" and "expensive as possible" are opposite ends of a sliding scale.

Private and public are also "sliding scale" opposites.[20] The scale's endpoints of the scale are "completely inaccessible to others" and "completely accessible to others."[21] To characterize privacy in public, we distinguish three regions on the scale: enclosure, obscurity, and voluntary restraint. The latter two comprise privacy in public. Both are ways in which people can

---

17. NIPPERT-ENG, *supra* note 10, at 4.

18. Idiomsfanatic, *You Can't Be Just a Little Bit Pregnant*, URBAN DICTIONARY, http://www.urbandictionary.com/define.php?term=you+can%27t+be+just+a+little+bit+pregnant (last visited Feb. 28, 2015); *see also Wall Street* (*1987 film*), WIKIPEDIA, http://en.wikipedia.org/w/index.php?title=Wall_Street_(1987_film)&oldid=649166214 (last visited Sept. 12, 2015).

19. *See generally Aristotle on Non-contradiction,* STAN. ENCYCLOPEDIA PHIL. (Feb. 22, 2007), http://plato.stanford.edu/entries/aristotle-noncontradiction/ ("An object can be potentially *F* and potentially not *F*, but it cannot be actually *F* and actually not *F* at the same time.").

20. NIPPERT-ENG, *supra* note 10, at 4 (noting that "[p]rivacy and publicity . . . are each defined with and by each other along [a] conceptual sliding scale").

21. *Id.*

ensure that others have no or limited access to information through their own efforts without relying on legal regulation. We do not mean to suggest that legal regulation is irrelevant to privacy in public. The point is simply that focusing on what people can do on their own provides a useful characterization of privacy in public.

A. ENCLOSURE

To enclose information is to surround it with a barrier that hinders others' access to it.[22] Houses and safes are examples. So are sealed letters—even though a bit of glue or tape is not much of a barrier. The seal is effective because opening another's mail violates social norms.[23] Houses and safes are similar. Both would offer less protection if it were socially acceptable to pick locks. The law of course also plays a role; it is, for example, illegal to open another's undelivered mail.[24] In general, the protection an enclosure provides is a function of the type of physical barrier, the relevant norms, and laws.[25] It would be interesting to explore the connections between norms laws and privacy by enclosure, but our concern is primarily with the two forms of privacy in public, obscurity and voluntary restraint.

B. OBSCURITY

Cities are a classic example of privacy by obscurity. As E. B. White famously observes, cities "bestow the gift of loneliness

---

22. The conception of privacy as enclosure is akin to Daniel Solove's "secrecy paradigm." According to that paradigm, "privacy is invaded by uncovering one's hidden world, by surveillance, and by the disclosure of concealed information." DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 8 (2004). The secrecy paradigm, however, has a much broader reach than privacy as enclosure. Enclosing information is only one way to kept it secret. As we explain below, obscurity and voluntary restraint can also ensure secrecy; thus, Solove's secrecy conception spans the distinctions we are drawing.

23. *See* ROBERT ELLIS SMITH, BEN FRANKLIN'S WEB SITE: PRIVACY AND CURIOSITY FROM PLYMOUTH ROCK TO THE INTERNET 24–26, 52–56 (2000); NIPPERT-ENG, *supra* note 10, at 70–71.

24. 18 U.S.C. § 1702 (2012) (criminalizing the "obstruction of correspondence").

25. *See generally* BRUCE SCHNEIER, LIARS AND OUTLIERS: ENABLING THE TRUST THAT SOCIETY NEEDS TO THRIVE (2012) (examining the role of trust and norms in ensuring security and privacy).

and the gift of privacy."[26] That gift also impressed the great nineteenth-century sociologist of urban life, Georg Simmel. He emphasized "the independence of the individual . . . in the dense crowds of the metropolis,"[27] and he noted that "under certain circumstances, one never feels as lonely and as deserted as in this metropolitan crush of persons."[28] The crush of persons made it possible for Edward Snowden to elude the United States in Hong Kong.[29] The city's "gift of privacy" allowed Snowden to elude the United States government while out in public.[30] Shifting "between several homes . . . [h]e was lost in a densely packed metropolis of seven million people."[31] As the city examples suggest, we will treat privacy by obscurity and privacy by enclosure as mutually exclusive. Simplicity is the reason. The borderline cases are interesting,[32] but there is no need to examine them here.

We focus on the fact that, as Woodrow Hartzog and Frederic Stutzman note in their seminal article on obscurity, "the concept of obscurity has languished in legal privacy doctrine."[33] The problem is that obscurity is generally equated with "hidden," and then dismissed as an unhelpful concept in privacy disputes.[34] Or, obscurity is conflated with other concepts such as confidentiality or the notion of "public information" and consequently overlooked as a distinct concept that could aid in the analysis of privacy disputes.[35] "The neglected and distorted state of obscurity in privacy doctrine is a significant problem because the concept of obscurity is too

---

26. E.B. WHITE, HERE IS NEW YORK 19 (The Little Bookroom 1999) (1949).

27. Georg Simmel, *The Metropolis and Mental Life*, *in* GEORG SIMMEL ON INDIVIDUALITY AND SOCIAL FORMS 324, 334 (Donald N. Levine ed., Edward Shills trans., Univ. of Chicago Press 1971) (1903).

28. *Id.*

29. HARDING, *supra* note 2.

30. *Id.*

31. *Id.* at 215–16.

32. Snowden in Hong Kong may be a borderline case—enclosure no doubt played some role in obscuring his location. *See id.*

33. Woodrow Hartzog & Frederic Stutzman, *The Case for Online Obscurity*, 101 CALIF. L. REV 1, 3 (2013). Our discussion of obscurity has benefitted greatly from their insightful examination of obscurity.

34. *Id*. at 17–18.

35. *Id.* at 40–41.

central to the expectations of Internet users for courts and lawmakers to ignore."[36]

One good way to show that obscurity is a distinct concept is to define it. Snowden's Hong Kong saga suggests an initial definition: information is obscure when it is not enclosed but still difficult to obtain.[37] Refining this proposal leads to an adequate characterization of privacy by obscurity.

The first refinement is to change difficult to difficult for a particular person in particular circumstances. To see the need, imagine you are attending a concert. You know a friend is too, but you cannot find her during the intermission. She is not enclosed. She is publicly observable, and is indeed being observed by others. Your problem is that her location is obscure. The crowd makes it difficult to find her. Difficult *for you*, that is—not for the people standing next to her. The current definition ignores the fact that what is difficult for one person may not be so for another. The solution is easy: information is obscure *for a person* when it is not enclosed but is still difficult *for that person* to obtain.[38]

Relativizing to persons is necessary but not enough. The reason: people differ in what they find difficult. Consider the *Where's Waldo?* books. The task is to find Waldo in a two page-spread packed with characters that look more or less like him.[39] Waldo is the only one in a red-and-white-striped shirt, bobble hat, and glasses, but the clutter of others makes him hard to see.[40] How hard depends on who is looking. The task can be daunting for an eight-year-old but easy for an adult, for whom finding Waldo just takes a little time and attention. Compare finding your friend at the concert. Time and attention

---

36. *Id.* at 3.

37. Technology has decreased the amount of privacy by obscurity in recent years. For example, today somebody carrying a powered-on smartphone with typical settings would not be obscure to the government even among Hong Kong's massive population. Snowden was careful not to do this. As another example, many US local government public records that were once available only in a myriad of scattered school district, township, county, etc. offices are now available online. HARDING, *supra* note 2; *see, e.g.*, SLOAN & WARNER, UNAUTHORIZED ACCESS, *supra* note 4 at 44 (discussing data mining and hidden information).

38. *See generally* Hartzog & Stutzman, *supra* note 33, at 18.

39. *See, e.g.*, MARTIN HANDFORD, WHERE'S WALDO? THE FANTASTIC JOURNEY (1989) (providing pictures of Waldo and instructions on how to locate him across the book).

40. *Id.*

may not be enough. Some means of finding your friend are unavailable—e.g., using a tracking device like Footprints installed on her phone.[41] She did not install the app, so you cannot use it to find her. Some means are available but unacceptable: for example, screaming her name at the top of your lungs, or (imagine you are an armed Secret Service agent) firing a gun into the air and then insisting that everyone line up for review. Some means may be available and acceptable, but cost too much. Suppose you want to find a friend in London with whom you have lost contact for years. Is the relevant information obscure for you? That depends on how much time, effort, and money you are willing to invest. You could hire a private investigator,[42] or try your hand at the detective work yourself.[43] It you are not willing to bear the cost, the information remains obscure to you.

What is the best way to accommodate these points about means in the definition of obscurity? We suggest changing "difficult" to "sufficiently difficult": information is obscure for a person provided that it is not enclosed, and it is *sufficiently* difficult for that person to obtain that information. Sufficiency is a *contextual* question. What counts as sufficient depends on available and acceptable means of obtaining the information in the circumstances, and the cost involved in employing those means in those circumstances (understand cost broadly to include not just monetary costs, but time, effort, and negative consequences). So will this do? Information is obscure for a person provided that it is not enclosed, and it is *sufficiently* difficult for that person to obtain that information.[44]

Not quite. Our examples are all lost-in-the-crowd cases,[45] but that is not the only way to make information obscure. Superman achieves obscurity through his disguise as Clark Kent.[46] Superman is not obscured by a crowd when he stands

---

41. *Find My Kids: Footprints*, FOOTPRINTS, http://www.footprints.net/ (last visited Sept. 12, 2015).

42. *Missing Persons*, HERITAGE INVESTIGATIONS, http://privateinvestigatorchicago.com/2012/missing-persons-chicago/ (last visited Sept. 12, 2015).

43. Using, for example, Google and sites like PeopleFinders. PEOPLEFINDERS, http://www.peoplefinders.com/ (last visited Oct. 16, 2015).

44. Hartzog & Stutzman, *supra* note 33, at 4.

45. As Woodrow Hartzog pointed out to us. *Id*.

46. LARRY TYE, SUPERMAN: THE HIGH-FLYING HISTORY OF AMERICA'S MOST ENDURING HERO 19 (2012).

in front of Lois Lane as Clark Kent; he is obscured by his disguise.[47] Compare disaggregated information. When it is aggregated, it can reveal a great deal even when no one piece or small collection is particularly revealing.[48] Should we think of the significance of the aggregated information as *lost in the crowd* or as *disguised*? Either answer is defensible. We opt for disguised. The idea is that the disaggregated information can stand right in front of you with its significance disguised by its disaggregated status. You could remove the disguise by obtaining more information, but you may not be able to afford the necessary time, effort, and money.

One final point remains. We have so far defined obscurity in terms of sufficient difficulty in *obtaining* information.[49] "Obtain" is ambiguous in ways we need to clarify. The Navajo code talkers of World War II are a good example. The "Navajo code talkers took part in every assault the U.S. Marines conducted in the Pacific from 1942 to 1945 . . . transmitting messages by telephone and radio in their native language, a code that the Japanese never broke."[50] The lack of understanding made the information obscure for them. They could still record it of course. So when they recorded the information, did they "obtain" it? The same question arises for encryption, a modern analogue of Navajo code talking.[51] Do people "obtain" information when they possess encrypted information they cannot decrypt? The answer is the same for both cases. Yes, if obtaining includes possessing information in a form you cannot make sense of it. No, if obtaining information requires possession and understanding. It is important to distinguish the two cases, and one good way to do

---

47. *Id.* (describing the creation and dynamic of the Clark Kent and Lois Lane relationship, "Lois who 'was ga-ga over super-powered Superman' and 'had an antipathy toward meek, mild Clark'").

48. *See* U.S. Dep't of Justice v. Reporters Comm. for Freedom of the Press, 489 U.S. 749, 763 (1989).

49. As Woodrow Hartzog pointed out to us. Hartzog & Stutzman, *supra* note 33.

50. Navy & Marine Corps WWII Commemorative Comm., *Navajo Code Talkers: World War II Fact Sheet*, NAVAL HIST. & HERITAGE COMMAND (May 19, 2004, 10:38 AM), http://www.history.navy.mil/browse-by-topic/diversity/native-americans-in-the-navy/navajo-code-talkers-world-war-ii-fact-sheet.html.

51. Conor Friedersdorf, *How Dangerous is Encryption*, ATLANTIC (July 14, 2015), http://www.theatlantic.com/politics/archive/2015/07/nsa-encryption-ungoverned-spaces/398423/.

that is to let "obtain" include "possess without understanding" and use "understand" for the "possess with understanding."

Thus our final definition of obscurity: Information is obscure for a person provided that it is not enclosed, and it is sufficiently difficult for that person to obtain or to understand that information.[52] Two essential points become clear against the background of this definition. The first is that privacy by obscurity is rapidly eroding.[53] It is a casualty of the surveillance practices we describe in the next section. Those practices greatly reduce the difficulty of both obtaining and understanding information.[54] The second point is that, even in full flower, privacy by obscurity would not give us all the privacy we need. The reason is that adequate privacy requires trusting others in ways that privacy by obscurity does not provide. The need for trust arises from the need to interact with others in ways that require revealing information to them.[55] Unless you can trust the others to handle that information in acceptable ways, you lose control over it and hence lose informational privacy. Privacy by obscurity provides no grounds for trusting others with one's information. Only the system of voluntary restraint does that.

---

52. *Compare* Woodrow Hartzog & Evan Selinger, *Obscurity: A Better Way to Think About Your Data than 'Privacy'*, ATLANTIC (Jan. 17, 2013), http://www.theatlantic.com/technology/archive/2013/01/obscurity-a-better-way-to-think-about-your-data-than-privacy/267283/ ("Obscurity is the idea that when information is hard to obtain or understand, it is, to some degree, safe. Safety, here, doesn't mean inaccessible. Competent and determined data hunters armed with the right tools can always find a way to get it. Less committed folks, however, experience great effort as a deterrent.").

53. Evan Selinger & Woodward Hartzog, *Obscurity and Privacy*, *in* THE ROUTLEDGE COMPANION TO PHILOSOPHY OF TECHNOLOGY 6–8 (Joseph Pitt & Ashley Shew eds., forthcoming).

54. *See generally The Internet Is a Surveillance State*, *supra* note 6 (claiming that everything we do or say on a computer is saved and can be accessed without warrant); DEIBERT, *supra* note 4 at 63 (explaining how private sector surveillance systems have access to "all of the data about us on social media"). *Contra* Ashlee Vance & Brad Stone, *Palantir, the War on Terror's Secret Weapon*, BUSINESSWEEK, (Nov. 22, 2011), http://www.businessweek.com/printer/articles/5771-palantir-the-war-on-terrors-secret-weapon (explaining how the large volume of information obtained by surveillance makes acquiring pertinent information exceedingly unlikely).

55. SCHNEIER, *supra* note 25 (examining the role of trust as necessary in a functioning society).

Our definition of obscurity is narrower than the one Hartzog and Stutzman offer. The difference is clear when they appeal to the sociologist Erving Goffman's *The Presentation of Self in Everyday Life*[56] to point out that "individuals both consciously and subconsciously attempt to 'produce' *obscurity* to protect their persons (defensively) or advance their goals (offensively)."[57] We agree that people attempt to produce *privacy*, but we distinguish two situations in which they do so, only one of which we categorize producing obscurity. In the first, a person succeeds in making it sufficiently difficult for others to obtain or understand information so that the information is obscure in the sense of our definition. The second situation is the one that impressed Simmel: people often voluntarily restrict the information they collect, use, and distribute.[58] They thereby ensure that certain information is private for purposes of the transaction even if it is public for other purposes. The information need not be difficult to obtain—at least not so difficult that it qualifies as obscure. People's voluntary restraint, nonetheless, keeps the information private for certain purposes even if it is public for others. We classify these cases separately as cases of voluntary restraint, not obscurity.[59]

Voluntary restraint promises privacy in public even in a world in which people store and exchange massive amounts of information by placing it in the hands of third parties—DropBox, social media sites, webmail systems, Google search histories, and the like. The information lacks obscurity since a variety of third parties typically have ready access to it and understand it.[60]

---

56. ERVING GOFFMAN, THE PRESENTATION OF SELF IN EVERYDAY LIFE (1959).

57. Hartzog & Stutzman, *supra* note 33, at 8 (emphasis added).

58. *See* Simmel, *supra* note 11.

59. Our disagreement with Hartzog and Stutzman may be more terminological than substantive. Like us, they assign norms a central role. They note that "our proposed definition and framework for online obscurity is based on Nissenbaum's [norm-based] theory of contextual integrity." Hartzog & Stutzman, *supra* note 33, at 19.

60. *Getting to Know You: Everything People Do Online Is Avidly Followed by Advertisers and Third-Party Trackers*, ECONOMIST, Sept. 13, 2014, at 5 (describing the thousands of third-party tracking firms that aggregate user data into detailed profiles that often reach levels of specificity beyond what advertisers can use). "Sometimes advertisers do not use information they have because they do not want to look as though they are spying on customers. 'We

C. VOLUNTARY RESTRAINT

Teachers and students in large universities are a good example. Teachers typically reveal little, if anything at all, about their personal lives to students, and they typically refrain from inquiring into students' personal lives. Students likewise limit what they reveal and what they ask. There are many exceptions (the Ph.D. student/dissertation supervisor relationship is sometimes one, for example),[61] but we focus on the general pattern. Limiting knowledge serves two important goals. The first is evaluating students only on the basis of relevant academic work. Limiting knowledge ensures that students appear to teachers primarily in the light of their relevant academic achievements, not in light of extracurricular aspects of their personalities, past academic records, honors conferred or punishments endured. The second goal is allowing teachers to model an intellectual or professional style that students can adopt and adapt in part because it is not tightly tied to a personal history.[62]

Similar remarks hold for a wide variety of interactions. Waiters do not try to find out whether you are married to your dinner partner, nor, if they know, announce that your partner is not your spouse. Your pharmacist does not ask if you are happy in your marriage when you pick up your Alprazolam

---

can do more technologically than we're permitted to culturally,' says Tony Weisman of DigitasLBi, a digital-advertising firm." *Id*.

61. Exceptions to informational norms are routine. *See* NIPPERT-ENG, *supra* note 10, at 108–09 ("[C]onceptual guidelines about what is private or public are only that. It is our ability to categorically stretch, contract, and otherwise elaborate or undermine these guidelines that creates a range of possible private-public classifications for every item, in every situation, across individuals. Cross-cultural differences and historical changes in social expectations regarding both of these categorical contents further complicate the story, of course. Indeed, participants' explanations of their piling decisions reveal quite a bit about the consistencies underlying individuals' conceptualizations of private and public. The privateness or publicness of an object also manifested in how people described handling it, especially during interactions with others.").

62. It is worth noting that limiting knowledge is not the only way to practice voluntary restraint. You may also limit your use and distribution of information. For example, suppose Schwartz knows that his student, Edwards, is a single parent who is working and going to school. He uses this information to make sure he encourages him to talk about the course in office hours, but he does not use it to favor him in grading, and he does not distribute the information to his colleagues without his consent.

(used for anxiety disorders),[63] but your internist may before he or she prescribes it. Waiters and restaurant patrons, students and teachers, pharmacists and customers, patients and doctors, and myriad others observe informational boundaries effortlessly, without thought or explicit negotiation. How does that happen?

Our answer appeals to informational norms. Informational norms

> circumscribe the type or nature of information about various individuals that, within a given context, is allowable, expected, or even demanded to be revealed. In medical contexts, it is appropriate to share details of our physical condition or, more specifically, the patient shares information about his or her physical condition with the physician but not vice versa; among friends we may pour over romantic entanglements (our own and those of others); to the bank or our creditors, we reveal financial information; with our professors, we discuss our own grades; at work, it is appropriate to discuss work-related goals and the details and quality of performance.[64]

Informational norms constrain the collection, use, and distribution of information.[65] The constraints vary as the relevant social roles vary.[66] Accordingly, we focus on informational norms that take this general form: people shall collect, use, and distribute information only in ways appropriate to their social roles.[67]

Return to teachers and students. Why do they voluntarily refrain from sharing certain information? Because it is an *informational norm* that teachers and students voluntarily refrain from sharing information in ways that ensure that students are evaluated, in each course, primarily in the light of their relevant academic achievements.

---

63. *Alprazolam*, MEDLINEPLUS, https://www.nlm.nih.gov/medlineplus/druginfo/meds/a684001.html (last updated Nov. 1, 2010).

64. Nissenbaum, *Privacy as Contextual Integrity*, *supra* note 10, at 138. Our emphasis on norms has its roots in Nissenbaum's work. We differ from Nissenbaum in the details of our conception of norms, in treating some informational norms as coordination norms, and in emphasizing the role of coordination norms in markets. *See* SLOAN & WARNER, UNAUTHORIZED ACCESS, *supra* note 4, at 95–120.

65. *See, e.g.*, Nissenbaum, *Privacy as Contextual Integrity*, *supra* note 10, at 132-33 (discussing shifting concepts of what constitutes private information).

66. *See, e.g.*, *id.* at 133–34 (discussing shifting concepts of privacy in the context of the home, public spaces, and the internet).

67. *See* SLOAN & WARNER, UNAUTHORIZED ACCESS, *supra* note 4, at 98–101 (discussing norm-appropriate uses of information based on social roles).

D. INFORMATIONAL NORMS AND COORDINATION

How do norms explain the coordination that creates privacy in public? In the same way that a norm explains why people in North America all drive on the right side of the road.[68] Safety and convenience dictate that you drive on the same side as everyone else, and you need to cooperate with all other drivers to do that.[69] In the United States and other "right side" countries, a norm enables and explains the coordination. Such norms are appropriately called *coordination norms*.[70] Driving on the right is in fact a classic example. The key feature is that people drive on the right because, and only as long as, almost everyone else does so.[71] The point is to realize the shared interest of all driving on the same side, so you would not drive on the right if you expected everybody else to drive on the left. The definition of a coordination norm is just a general characterization of this sort of pattern. Thus: a coordination norm is a behavioral regularity in a group, where the regularity exists at least in part because (almost) everyone thinks that, in order to realize a shared interest, she ought to conform to the regularity, as long as everyone else does.[72] Entering an elevator is another good example. The norm is to maximize the distance to your nearest neighbor.[73] All share an

---

68. *See* Richard F. Weingroff, *On the Right Side of the Road*, U.S. DEP'T OF TRANSP. (Oct. 17, 2013), https://www.fhwa.dot.gov/infrastructure/right.cfm (noting that the history of right-handed and left-handed travel is based on customs).

69. Edna Ullman-Margalit, *Coordination Norms and Social Choice*, 11 ERKENNTNIS 143, 147 (1977).

70. *Id.*

71. *See, e.g.*, H. Peyton Young, *The Economics of Convention*, 10 J. ECON. PERSPECT. 105, 107–08 (1996) (providing a game-theoretic explanation of the decision made by individual drivers as to whether to drive on the right or left side of the road).

72. *See* SLOAN & WARNER, UNAUTHORIZED ACCESS, *supra* note 4, at 56–59; *see also* ELINOR OSTROM, UNDERSTANDING INSTITUTIONAL DIVERSITY 112 (2005) ("As discussed in some detail in chapter 5, norms can be thought of as shared concepts of what must, must not, or may be appropriate actions or outcomes in particular types of situations."); Ullman-Margalit, *supra* note 69.

73. This is a simplification. The true norm is would be to maximize the distance to your nearest neighbor but also stay within the peripheral vision of at least one other passenger, and keep at least one other passenger within your own peripheral vision. *See* JAMES S. SMITH, THE TREASURE HUNT: DISCOVER AND RECLAIM YOUR LIFE 71 (2012) (discussing the norm of establishing a maximum distance when other passengers enter the elevator); Janine Driver, *The Unwritten Rules of Elevator Etiquette*, TODAY HEALTH

interest in being able to use the elevator while not being overcrowded. No one can realize the interest unilaterally, and elevator users think they ought to conform to achieve this balance—as long as everyone else does so. If everyone else just stands anywhere they like, being a nearest-neighbor distance maximizer does not prevent overcrowding.

Not all informational norms are coordination norms,[74] but the ones that concern us are. The coordination they facilitate creates privacy in public through mutual voluntary restraint. We conclude with two examples, both of which figure later in our discussion of governmental surveillance.

The student/teacher norm is the first example.[75] It fulfills the conditions for a coordination norm. First, there is a shared interest. Students and teachers share an interest in evaluating students primarily for relevant academic work and in teachers being evaluated primarily for teaching effectiveness. Second, neither students nor teachers can realize that interest unilaterally. Each group must voluntarily refrain from revealing and learning too much. Third, the commitment to such restraint is conditional. It takes a critical mass of information-restricting students and teachers to ensure that students and teachers are evaluated only on the basis of appropriate information. There is no "ensuring appropriate academic evaluation" point to being an information-restricting student or teacher unless enough others are, so teachers and students will typically honor the commitment only if enough others do.

(Aug. 18, 2007, 10:54:05 AM), http://www.today.com/id/20335786/ns/today-today_health/t/unwritten-rules-elevator-etiquette (same); Rebekah Rousi, *An Uplifting Experience – Adopting Ethnography to Study Elevator User Experience*, ETHNOGRAPHY MATTERS (Apr. 2, 2013), http://ethnographymatters.net/blog/2013/04/02/an-uplifting-experience-adopting-ethnography-to-study-elevator-user-experience/ (discussing how behaviors surrounding spacing and eye-contact while riding elevators vary between a building with a front security desk and a building without a front security desk).

74. As previously discussed in Warner & Sloan, *Self, Privacy, and Power*, *supra* note 7, at 82 n.68, "Make your comments relevant" is an informational norm but not a coordination norm. The hallmark of a coordination norm is that you adhere to it *only* as long as others do, but you would adhere to the relevant comment norm even if most others did not.

75. For a similar discussion of the example of student/teacher relationships in the context of coordinating norms around privacy, see *id.* at 71, 78–79.

Journalists and their sources are the second example. The norm is that, exceptional circumstances aside, journalists protect the political independence of the press by not revealing their confidential sources.[76] The argument that this norm is a coordination norm parallels the student/teacher case. There is a relevant shared interest. Journalists share an interest in maintaining the secrecy of whistleblowing sources to ensure that journalism plays an effective role as a political watchdog.[77] No journalist can realize the interest unilaterally. No single journalist can ensure a politically independent press. That takes a concerted effort of a critical mass of journalists as well as editors and media owners plus an appropriate political system and culture. Finally, the commitment to non-disclosure is conditional. That follows from the "critical mass" point. If not enough journalists will refuse to disclose their confidential sources, then there is no "ensuring the independence of the press" justification for submitting yourself to the harassment of

---

76. *See, e.g.*, Adam Liptak, *Reporter Jailed After Refusing to Name Source*, N.Y. TIMES, July 7, 2005, at A1 (reporting on New York Times reporter Judith Miller's initial refusal to disclose a confidential source to a grand jury, telling federal judge Thomas F. Hogan "if journalists cannot be trusted to guarantee confidentiality, then journalists cannot function and there cannot be a free press").

77. *See, e.g.*, Commissioner for Human Rights, Council of Europe, *Ethical Journalism and Human Rights* (Nov. 8, 2011), https://wcd.coe.int/ViewDoc.jsp?id=1863637#P252_37545 ("When courts and public authorities ask journalists to hand over material or information that may reveal a source of information, most reporters will instinctively demur but occasions arise when journalists come to a different ethical conclusion and their conscience compels them to co-operate with the authorities, as some did by giving evidence at the International Criminal Tribunal for the former Yugoslavia in The Hague . . . . Ethical reporting does not require a legal framework—although journalists who practise it do need the law to guarantee their rights to work freely—but to build credibility and public confidence journalism must adhere to codes of conduct and norms of ethical behaviour."); *see also* BOGHOSIAN, *supra* note 4, at 183 ("Most journalists feel an obligation to protect their confidential sources even if threatened with jail time."); Leighton Walter Kille, JOURNALIST'S RESOURCE (Nov. 26, 2009), http://journalistsresource.org/tip-sheets/foundations/principles-of-journalism ("Journalism has an unusual capacity to serve as watchdog over those whose power and position most affect citizens. The Founders recognized this to be a rampart against despotism when they ensured an independent press; courts have affirmed it; citizens rely on it."); Stephen J.A. Ward, *Why Hyping Transparency Distorts Journalism Ethics*, MEDIASHIFT (Nov. 4, 2013), http://www.pbs.org/mediashift/2013/11/why-hyping-transparency-distorts-journalism-ethics/.

government surveillance,[78] the risk of imprisonment for refusal to disclose a source, [79] and, in national security cases, the possible threat of prosecution under the Espionage Act.[80]

There are many similar examples.[81] Our claim is that governmental surveillance can, and does, undermine the norm-based coordination on which privacy in public depends. One good reason this matters is that adequate self-realization requires adequate privacy in public.

II. PRIVACY IN PUBLIC AND THE SELF

We make three claims.[82] First, the realization of a multifaceted self is a personal and political ideal. Second, you realize such a self in large part through social roles that mediate interactions with others. Third, such realization requires a significant degree of privacy in public. We argue for each claim in turn.

A. THE IDEAL OF A MULTIFACETED SELF

We begin with William James. "I am," James writes,

> often confronted by the necessity of standing by one of my . . . selves and relinquishing the rest. Not that I would not, if I could, be both handsome and fat and well dressed, and a great athlete, and make a million a year, be a wit, a *bon-vivant*, and a lady-killer, as well as a philosopher; and a philanthropist, statesman, warrior, and African explorer, as well as a 'tone poet' and saint. But the thing is simply impossible . . . . Such different characters may conceivably at the outset of life be alike *possible* to a man. But to make any one of them actual, the rest must more or less be suppressed. So the seeker of his truest, strongest, deepest self must review the list carefully, and pick out the one on which to stake his salvation.[83]

---

78. *See, e.g.*, The Editorial Board, *Spying on the Associated Press*, N.Y. TIMES, MAY 14, 2013, at A24.

79. *See, e.g.*, Liptak, *supra* note 76.

80. RAHUL SAGAR, SECRETS AND LEAKS: THE DILEMMA OF STATE SECRECY 105, 154–55 (2013).

81. We have analyzed a number of other examples elsewhere. SLOAN & WARNER, UNAUTHORIZED ACCESS, *supra* note 4.

82. As presented previously in Warner & Sloan, *Self, Privacy, and Power*, *supra* note 7, at 64–65 (presenting the multifaceted self in three similar claims to discuss the relation between self, privacy, and the private sector's control of our online activity).

83. 1 WILLIAM JAMES, THE PRINCIPLES OF PSYCHOLOGY 309–10 (photo reprint 1950) (1890).

"You make yourself who you are by what you 'stand by,' by the commitments you strive to realize."[84] We take this to be a widely shared conception of the self—with one emendation. James is wrong when he suggests that *one* central commitment defines who you are; instead, as John Gray notes,

> We are none of us defined by membership in a single community or form of moral life. We are . . . heirs of many distinct, sometimes conflicting, intellectual and moral traditions . . . . The complexity and contradictions of our cultural inheritance give to our identities an aspect of complexity and even of plurality which is . . . essential to them . . . . [T]he power to conceive of ourselves in different ways, to harbour dissonant projects and perspectives, to inform our thoughts and lives with divergent categories and concepts, is integral to our identity as reflective beings.[85]

The self you seek to realize is a *multifaceted* self. People differ of course both in how much multiplicity they seek and in how assiduously they try to realize that multiplicity, but, subject to those differences, the realization of a multifaceted self is a widespread personal ideal.[86]

---

84. Richard Warner, *Adjudication and Legal Reasoning*, *in* THE BLACKWELL GUIDE TO THE PHILOSOPHY OF LAW AND LEGAL THEORY 259, 269 (Martin P. Golding & William A. Edmundson eds., 2005). As previously noted in Warner & Sloan, *Self, Privacy, and Power*, *supra* note 7, at 67 n.21, there is more than one candidate for the label "concept of the self." In particular, there are "pure ego" or "center" theories. *See* C.D. BROAD, THE MIND AND ITS PLACE IN NATURE 278, 558–62, (photo. reprint 2009) (1925); COLIN MCGINN, THE CHARACTER OF MIND: AN INTRODUCTION TO THE PHILOSOPHY OF MIND 140–62 (2d ed. 1997). For a commitment-based theory of the self, see RICHARD WARNER, FREEDOM, ENJOYMENT, AND HAPPINESS: AN ESSAY ON MORAL PSYCHOLOGY 92–99 (1987).

85. JOHN GRAY, POST-LIBERALISM: STUDIES IN POLITICAL THOUGHT 262–63 (1993). It is not clear that James actually disagreed. As he notes elsewhere,

> [p]roperly speaking, *a man has as many social selves as there are individuals who recognize him* and carry an image of him in their mind . . . Nothing is commoner than to hear people discriminate between their different selves of this sort: "As a man I pity you, but as an official I must show you no mercy; as a politician I regard him as an ally, but as a moralist I loathe him;" etc., etc.

JAMES, *supra* note 83, at 294–95.

86. Steven L. Blader, *Let's Not Forget the "Me" in "Team": Investigating the Interface of Individual and Collective Identity*, *in* IDENTITY AND THE MODERN ORGANIZATION 61, 64–65 (Caroline A. Bartel et al. eds., 2007) (noting that in psychological research, "[t]he research evidence supporting distinctions among various levels of self construal is extensive" and widespread with variation among researchers looking at different emphasis and interactions between levels from the individual self up to the collective self).

This conception of the self also underlies liberal political philosophy,[87] the tradition in which we place ourselves. The traditional political ideal is that the state should ensure, if not actual self-realization, at least adequate *opportunity* to realize a multifaceted self.

B. SOCIAL ROLES

Social roles mediate self-realization.[88] You could not, for example, be a journalist in a society that does not recognize that role. Try to imagine the opposite. Imagine you live in a society in which magazines, news media, and the like do not exist. You are the lone deviant who does the things that journalists do in other societies. You regularly investigate events, collect and analyze material, and conduct interviews. You do so with the primary intention of informing the public on a variety of issues you find important. You are still not a journalist in the sense that, for example, Bob Woodward is.[89] To be a journalist in that sense is to fulfill a *recognized role*. Contemporary society recognizes that behavior pattern as a vocation, not as deviant and bizarre, and this means that Woodward can refer to this role to explain his activities to himself and other others. You cannot do that. You are just deviant.

Similar examples abound. You cannot be a whistleblower, an undercover agent, or university professor except in a society with the appropriate institutions and practices. Even being a parent, child, lover, or spouse takes on different meanings and definitions depending on the society in which the relationship is realized.[90]

---

87. For an excellent overview, see John Christman, *Autonomy in Moral and Political Philosophy*, STAN. ENCYCLOPEDIA PHIL. (Aug. 11, 2009), http://plato.stanford.edu/archives/spr2011/entries/autonomy-moral/.

88. *See* JOSEPH RAZ, THE MORALITY OF FREEDOM 307–13, 348–57 (1986) (emphasizing the importance of social roles—what he calls "social forms"—to the development of the self).

89. *See generally Full Biography*, BOB WOODWARD, http://bobwoodward.com/full-biography (last visited Oct. 1, 2015).

90. As we have previously discussed in Warner & Sloan, *Self, Privacy, and Power*, *supra* note 7, at 69 & n.30, to avoid misunderstanding, we should emphasize that we are not saying that one's possibilities or self-realization are *completely* circumscribed by available social roles. Suppose that you live in a yet to be discovered primitive tribe, isolated from the rest of the world. Women are generally regarded as fungible property to be bought and sold. You are the sole voice for gender equality. While the tribe recognizes other applications of

C. THE NEED FOR PRIVACY IN PUBLIC

Realizing a multifaceted self means realizing multiple social roles, and that requires privacy in public.[91] Perhaps the most obvious reason is that combining roles may violate others' expectations. Consider: parent and gay or lesbian;[92] politician and explorer of sexuality in sex clubs;[93] exemplary elementary school teacher and connoisseur of legal pornography; FBI agent and whistleblower.[94] The consequences of disappointing others'

---

the concept of equality, gender equality seems ludicrous at best, unintelligible at worst. Neither you, nor your society can understand your gender equality claims with reference to a *recognized social role*, at least not the role of "advocate for gender equality." *You*, however, can still understand yourself as committed to gender equality and that commitment can play a central role in your self-definition. You are just extending your society's notion of equality into a new area. Such examples do not, however, undermine our point that for the most part the roles through which one realizes a multifaceted self are social roles recognized in the society in which one lives.

91. For a similar discussion of privacy in public as it relates to norms and expectations, see Warner & Sloan, *Self, Privacy, and Power*, *supra* note 7, at 69–73.

92. Alana Semuels, *Should Adoption Agencies Be Allowed to Discriminate Against Gay Parents?*, ATLANTIC (Sept. 23, 2015), http://www.theatlantic.com/politics/archive/2015/09/the-problem-with-religious-freedom-laws/406423/ ("[S]ome people don't think gay couples should be allowed to foster or adopt children.").

93. *See* Sarah Hall, *Jeri Ryan Sex-Club Scandal*, E! ONLINE (June 22, 2004), http://www.eonline.com/news/47694/jeri-ryan-s-sex-club-scandal. As discussed previously in Warner & Sloan, *Self, Privacy, and Power*, *supra* note 7, at 69 & n.32, Jack Ryan's desire to explore sex with his famous actress wife Jeri Ryan in a sex club may have been responsible for President Obama's election to the US Senate in 2004. Ryan had won the Republican primary for that Senate race and appeared to have a reasonable chance of defeating Obama in the general election—until the news about the sex club broke. Ryan was forced to withdraw from the race, and the Republican party of Illinois selected the relative unknown Alan Keys to replace Ryan. Dan Collins, *Sex Scandal Ends Ryan Senate Bid*, CBS NEWS (June 25, 2004), http://www.cbsnews.com/news/sex-scandal-ends-ryan-senate-bid/; *Obama wins Senate Race to Become 5th Black U.S. Senator in History*, USA TODAY (Nov. 2, 2004), http://usatoday30.usatoday.com/news/politicselections/vote2004/2004-11-02-il-ussenate_x.htm. Obama went on to win the general election in a landslide.

94. Coleen Rowley was an FBI agent who disclosed a memo she wrote to the Director of the FBI explaining how FBI headquarters in Washington had hindered her investigation of Zacarias Moussaoui, an investigation that might have prevented the 9/11 attacks. *Time Magazine* named her as a person of the year for 2002, but facing what she described as a nasty backlash from the FBI, she resigned from the FBI in 2004 after 24 years as an agent. *See* SAGAR, *supra* note 80, at 148.

expectations can range from disapproval, to reprisal, to ostracism.

Avoiding disapproval and reprisal are not, however, the only reasons to seek privacy in public. Imagine, for example, that you eat frequently in a small Italian trattoria. You want to play the role of "customer they know very little about" in order to have an experience as disconnected as possible from the rest of your life. You want a pleasant break from that life. Your concern is not with their approval or disapproval; it is just with what they know. You do not merely care that more knowledge would change the way they relate to you. You do not want to have even to *think* about whether it *might* do that. The restaurant example illustrates two key points. First, social roles are typically *defined* in part by the way you appear to others when you are in them. Second, how you appear to others depends on what those others know. The student/teacher and journalist/confidential source examples illustrate the same two points. The parties in those relationships cannot fulfill those roles without the control over how they appear.

Control over how you appear to the government is an important component of the control over appearance required for successful self-realization. People play a wide variety of roles in relation to the government, including: dissident, political activist, member of the Sierra Club, academic critic of the government, anonymous political critic, member of the Democratic or Republican party, politically uninvolved, and so on. How you appear to the government has a profound impact on your prospects for self-realization. Some, for example, long to take center stage in support of, or in opposition to, the government; for others, that would be their worst nightmare.

In general, different requirements on what one is allowed, expected, or required to reveal or not reveal define different relationships with governmental authorities, acquaintances, colleagues, friends, family, employers, and so on.[95] The point is a familiar one in sociology. As the sociologist Nippert-Eng emphasizes:

> At its core, managing privacy is about managing relationships between the self and others . . . . [P]rivacy . . . [is] a "boundary regulatory process by which a person (or group) makes himself more or less accessible and open to others." When we regulate our accessibility to others, though—including the accessibility of

95. Warner & Sloan, *Self, Privacy, and Power*, *supra* note 7, at 73.

> information, objects, space, time, or anything else that we deem private—we simultaneously regulate our relationships with them.[96]

"Secrecy," she explains, "is a means to an end, a process in which we actively work to manage our private matters."[97] Indeed,

> No matter what the secret, no matter how it is manipulated or what its fate, to consider a secret is to simultaneously consider the relationships (perhaps entire social networks) that it throws into relief. Indeed, from a sociological perspective, perhaps the most significant aspect of secrets is their selectively shared nature. There are secrets *with* and secrets *from*, intentionally disclosed to and concealed from specific individuals at specific times and in specific ways. Simultaneously inclusive and exclusive, secrets are quite effective at achieving social boundary work, an excellent measure of the social distance between individuals.[98]

Section IV argues that the government's current surveillance practices can undermine the norm-based coordination required for privacy in public and thus can seriously curtail self-realization. Section III provides essential background.

III. SURVEILLANCE CONCEPTS

Examinations of governmental surveillance typically concentrate on the use of surveillance information to discourage or prevent behavior that the government finds undesirable.[99] We consider five aspects of surveillance: knowledge, use, merely knowing, complicity, and uncertainty. In the next section, we show how these five features combine to undermine privacy in public.

A. KNOWLEDGE

We will use "know" and "knowledge" in an artificially broad sense. One of Snowden's remarks illustrates our use and rationale: "I, sitting at my desk, could wiretap anyone, from you or your accountant, to a federal judge or even the

---

96. NIPPERT-ENG, *supra* note 10, at 22 (quoting IRWIN ALTMAN, THE ENVIRONMENT AND SOCIAL BEHAVIOR: PRIVACY, PERSONAL SPACE, TERRITORY, CROWDING 3 (1975)). Charles Fried offers a similar conception in Charles Fried, *Privacy*, 77 YALE L.J. 475 (1968).

97. NIPPERT-ENG, *supra* note 10, at 24 (footnotes omitted).

98. *Id.* at 27 (footnotes omitted).

99. *See infra* Section III, B.

president, if I had a personal email."[100] He was referring evidently to the National Security Agency's (NSA) XKeyscore program which "allows analysts to search . . . through vast databases containing emails, online chats and the browsing histories of millions of individuals."[101] Imagine XKeyscore's databases include the fact that you recently purchased Susan Landau's *Surveillance or Security?*: *The Risks Posed by New Wiretapping Technologies*.[102] Does that mean Snowden knows you bought the book? Of course not. He *could find out* from XKeyscore that you did, but until he discovers that fact, he does not know. We use "know" more broadly: the government *knows* a fact when it possesses information that would reveal that fact *even if no person has examined the information and thereby reached that conclusion*.[103] The point is convenience.

---

100. *See* Glenn Greenwald, *How NSA Can See 'Nearly Everything You Do Online': Secret Tool Searches Email, Chat and Social Media Use*, GUARDIAN, Aug. 1, 2013, at 1.

101. *Id.* For an accurate, well-documented summary of XKeyscore, see *XKeyscore*, WIKIPEDIA, http://en.wikipedia.org/w/index.php?title=XKeyscore&oldid=620306883 (last visited Oct. 16, 2015). For a discussion that sets XKeyscore in context, see *INCENSER, or How NSA and GCHQ Are Tapping Internet Cables*, TOP LEVEL COMM. (Nov. 29, 2014), http://electrospaces.blogspot.de/2014/11/incenser-or-how-nsa-and-gchq-are.html.

102. LANDAU, *supra* note 4.

103. One source of our concern to be clear about our sense of "know" is the infamous exchange between Senator Ron Wyden and Director of National Intelligence James Clapper. Wyden asked Clapper, "Does the NSA collect any type of data at all on millions or hundreds of millions of Americans?" Dan Amira, *Is This a Video of the Director of National Intelligence Lying to Congress? [Updated]*, N.Y. MAG.: DAILY INTELLIGENCER (June 6, 2013, 5:13 PM), http://nymag.com/daily/intelligencer/2013/06/wyden-clapper-nsa-video-congress-spying.html. Clapper's reply was, "No, sir ... not wittingly." *Id.* Clapper was accused of lying when Snowden's documents revealed the NSA's practice of "bulk surveillance, the NSA's collection of everything it can obtain on every communications channel to which it can get access. This includes things such as the NSA's bulk collection of call records, location data, e-mail messages and text messages." Bruce Schneier, *It's Time to Break Up the NSA*, SCHNEIER ON SECURITY (Feb. 20, 2014), https://www.schneier.com/essays/archives/2014/02/its_time_to_break_up.html. As Bruce Schneier noted, "[Clapper's] definition of 'collect' requires that a human look at it. So when the NSA collects—using the dictionary definition of the word—data on hundreds of millions of Americans, it's not *really* collecting it, because only computers process it." Bruce Schneier, *Why the NSA's Defense of Mass Data Collection Makes No Sense*, ATLANTIC (Oct. 21, 2013), http://www.theatlantic.com/politics/archive/2013/10/why-the-nsas-defense-of-mass-data-collection-makes-no-sense/280715/. See ADMINISTRATION WHITE PAPER: BULK COLLECTION OF TELEPHONY METADATA UNDER SECTION 215 OF THE USA PATRIOT ACT

The governmental *capacity* to know is our concern, and it makes for easier reading if we can just talk about what the government knows without having to always insert the qualification that we mean the capacity to know. One more qualification: the government does not always *know*, sometimes it merely believes and indeed may mistakenly believe.[104] To avoid having to always say "know or believe," we will use "know" to cover the belief cases as well.

Knowledge requires access to information. The government ensures access in three ways: data collection, aggregation/distribution, and the public/private surveillance partnership. We discuss each in turn.

1. Data Collection

The window Snowden opened on the NSA has made it the sinister poster child for those concerned about governmental surveillance.[105] His disclosures—totaling over 6,000 pages as of Fall 2015[106]—reveal the astonishingly wide reach of the NSA's data collection.[107] In the NSA's own words: "Collect it All; Process it All; Exploit it All; Partner it All; Sniff it All; Know it All."[108] A comparison with the Stasi highlights the extent of the

---

(2013) [http://perma.cc/8RJN-EDB7], for the Government's justification for its data collection program.

104. *E.g.*, Ana Garcia & Fred Mamoun, *Mistakes on "No Fly List" Keeping Travelers Grounded*, NBC L.A. (Nov. 6, 2009, 2:23 PM), http://www.nbclosangeles.com/on-air/as-seen-on/Mistakes-on-No-Fly-List-Keeping-Travelers-Grounded-69337037.html ("[P]roblems checking-in persist for Garcia and many other Americans who have been erroneously placed on the watch list.").

105. *See, e.g.*, Dustin Volz, *Edward Snowden Is Concerned About 'NSA Fatigue'*, DEFENSE ONE (Aug. 14, 2015), http://www.defenseone.com/technology/2014/08/edward-snowden-concerned-about-nsa-fatigue/91496/.

106. *Snowden Tally*, CRYPTOME, http://cryptome.org/2013/11/snowden-tally.htm (last visited Oct. 16, 2015).

107. For the reach of the NSA's surveillance, see Jody Avirgan, *A Running List of What We Know the NSA Can Do. So Far.*, WNYC (Jan. 17, 2014), http://www.wnyc.org/story/running-list-what-we-know-nsa-can-do-so-far/.

108. That was the NSA's description of its ambitions in a PowerPoint slide at a secret meeting of the Five Eyes Alliance. Andrew Conry Murray, *Collect It All: The NSA Surveillance Doctrine*, INFORMATIONWEEK (Aug. 1, 2014, 12:00 AM), http://www.informationweek.com/interop/collect-it-all-the-nsa-surveillance-doctrine/a/d-id/1297748. The "five eyes" are Britain, the United States, Australia, New Zealand, and Canada. Paul Farrell, *History of 5-Eyes – Explainer*, GUARDIAN (Dec. 2, 2013, 12:30 AM), http://www.theguardian.com/world/2013/dec/02/history-of-5-eyes-explainer.

NSA's data collection.[109] "What is remarkable about the Stasi is its penetration of the most ordinary, ostensibly nonthreatening, areas of East Germany."[110] As a former Stasi agent put it, "'[t]here was nothing that we weren't interested in.'"[111] The Stasi "monitored 2,800 postal addresses; the agency steamed 90,000 letters a day."[112] It also used a large informant network. "[I]n 1989, there were precisely 91,015 full-time Stasi employees and 173,000 informants."[113] This translates into roughly 1 in 50 East Germans working for the Stasi.[114] The NSA's data collection regime exceeds the Stasi's wildest dreams.[115] According to Foreign Intelligence Surveillance Court Judge Bates, the "NSA acquires more than *two hundred fifty million* Internet communications each year."[116] The estimate may be quite low. Greenwald reports that Snowden's documents show that "for a thirty-day period ending in February 2013, one unit of the NSA collected more than *three billion* pieces of communication data from US communication systems alone."[117]

As astonishing as the NSA's data collection practices are, they are consistent with past practices. The technologies are new, but the practices are of a piece with governmental surveillance in the United States from the Franklin Roosevelt Administration on.[118] Indeed, the twentieth century and the

---

109. *See generally* Elizabeth Murray, *Examining the Stasi, Seeing the NSA*, CONSORTIUMNEWS (Feb. 3, 2015), https://consortiumnews.com/2015/02/03/examining-the-stasi-seeing-the-nsa/.

110. BRUCE, *supra* note 1, at 11.

111. *Id.* at 55.

112. HARDING, *supra* note 2, at 254.

113. BRUCE, *supra* note 1, at 10.

114. *Id.* at 10 & 190 n.45.

115. *See generally* Ray Pensador, *Worse Than the Stasi: How the Corporate State is Turning Citizens into Spies*, DAILY KOS (Dec. 17, 2013, 11:53 AM), http://www.dailykos.com/story/2013/12/17/1263418/-Worst-Than-The-Stasi-How-The-Corporate-State-is-Turning-Citizens-Into-Spies.

116. Memorandum Opinion of Oct. 3, 2011, 2011 WL 10945618, at *9 (FISA Ct., Oct. 3, 2011) (emphasis added). Judge Bates notes that "the Court cannot know for certain the exact number of wholly domestic communications acquired through this collection, nor can it know the number of non-target communications acquired or the extent to which those communications are to or from United States persons or persons in the United States." *Id.* at *10.

117. Greenwald, *supra* note 4, at 30.

118. Theoharis provides a detailed and well-documented account of the growth of governmental surveillance from the 1933 Roosevelt Administration to the present. *See generally* THEOHARIS, *supra* note 4.

beginning of the twenty-first show a pattern of increasingly pervasive and sophisticated surveillance by federal, state, and local governments.[119] Consider federal, state, and city video and photo surveillance. Among cities, Chicago leads a large pack. With 20,000 video cameras in "downtown Chicago, virtually every segment of the public way is under constant video surveillance."[120] The system also incorporates "NeoFace, one of the facial-recognition tools being used by police departments across the country."[121]

Video surveillance is just one of a number of widely used surveillance technologies. Others include, to name just a few, remote fingerprint scanners,[122] laser scanners that can "penetrate clothing and many other organic materials,"[123] and palm and iris scanners.[124] Our discussion of data collection barely scratches the surface, but it should suffice to underscore the fact that the government collects, and is deeply committed to collecting, a massive amount of data.

---

119. As Theoharis notes, "Roosevelt's unprecedented authorization of Federal Bureau of Intelligence (FBI) 'intelligence' investigations, combined with the similarly secret authorization . . . of other preventive detention and informer programs, . . . shifted the focus of FBI investigations from law enforcement to monitoring the political and personal activities of suspected 'subversives.'" *Id.* at 24.

120. Adam Schwartz, *Chicago's Video Surveillance Cameras: A Pervasive and Poorly Regulated Threat to Our Privacy*, 11 NW. J. TECH. & INTELL. PROP. 47, 47 (2013). Operation Virtual Shield integrates the cameras into an information processing and analysis system, which can, for example, "automatically search for the image of a particular car, and then automatically track its movements, following the car out of the range of one camera and into the range of the next." *Id.* at 49–50; *see also* Frank Main, *Chicago police go high-tech with facial recognition software*, CHI. SUN-TIMES (July 13, 2013, 10:08 AM) [http://web.archive.org/web/20141210013713/http://www.suntimes.com/21268770-761/chicago-police-go-high-tech-with-facial-recognition-software.html#.VhLIKMtVhBc].

121. Main, *supra* note 120; *see* BILGE YESIL, VIDEO SURVEILLANCE POWER AND PRIVACY IN EVERYDAY LIFE 6–7, 28–29 (2009); *Intellistreets*, ILLUMINATING CONCEPTS, http://www.illuminatingconcepts.com/intellistreets/ (last visited Sept. 13, 2015); *Chicago Police Start Using Facial-Recognition Software to Arrest Suspects*, RT (Jul. 15, 2013, 9:29 PM), http://rt.com/usa/chicago-police-cctv-surveillance-135/.

122. *See, e.g.*, IDAIR, http://www.idairco.com/ (last visited Oct. 16, 2015).

123. *E.g.*, *Hidden Government Scanners Will Instantly Know Everything About You From 164 Feet Away*, GIZMODO (Jul. 10, 2012, 9:40 AM), http://gizmodo.com/5923980/the-secret-government-laser-that-instantly-knows-everything-about-you.

124. *See, e.g.*, IRIS ID, http://www.irisid.com/ (last visited Oct. 16, 2015); BLINKSPOT, http://www.blinkspot.com/ (last visited Oct. 16, 2015).

2. Aggregation and Distribution

Data aggregation and distribution take what separate entities know and combine and distribute it so that many more know it.[125] Palantir is a good example. Palantir, funded in its startup phase by the venture capital arm of the CIA,[126] is a private business that sells "a suite of software applications for integrating, visualizing and analyzing the world's information. [It] support[s] many kinds of data including structured, unstructured, relational, temporal and geospatial."[127] The software allows you to access and make sense of data scattered across any number of different databases.[128] It can tie "together surveillance video . . . with credit-card transactions, cell-phone call records, e-mails, airplane travel records, and Web search information."[129] Palantir "has built a customer list that includes the U.S. Defense Dept., CIA, FBI, Army, Marines, Air Force, the police departments of New York and Los Angeles, and a growing number of financial institutions trying to detect bank fraud."[130]

Here is how it works. Mike Fikri gets a speeding ticket on his way to Orlando, Florida.[131] The ticket sets off an alert in the CIA's Palantir system, prompting an analyst to search for data.[132] A graphical user interface displays the results: finger print and DNA evidence collected in Cairo; an ATM video from

---

125. Data Aggregation, WIKIPEDIA, https://en.wikipedia.org/wiki/Data_aggregation (last visited Oct. 16, 2015).

126. Andy Greenberg & Ryan Mac, *How A 'Deviant' Philosopher Built Palantir, A CIA-Funded Data-Mining Juggernaut*, FORBES (Aug. 14, 2013, 9:10 AM), http://www.forbes.com/sites/andygreenberg/2013/08/14/agent-of-intelligence-how-a-deviant-philosopher-built-palantir-a-cia-funded-data-mining-juggernaut/.

127. Palantir Technologies, IN-Q-TEL, https://www.iqt.org/iqt_portfolio/palantir-technologies/ (last visited Oct. 16, 2015).

128. Palantir Gotham, PALANTIR TECHNOLOGIES, https://www.palantir.com/palantir-gotham/ (last visited Oct. 16, 2015).

129. Ashlee Vance & Brad Stone, *Palantir, the War on Terror's Secret Weapon*, BUSINESSWEEK (Nov. 22, 2011), http://www.businessweek.com/printer/articles/5771-palantir-the-war-on-terrors-secret-weapon.

130. *Id.*; *see also* Greenberg & Mac, *supra* note 126 ("Palantir lives the realities of its customers: the NSA, the FBI and the CIA–an early investor through its In-Q-Tel venture fund–along with an alphabet soup of other U.S. counterterrorism and military agencies.").

131. Fikri is a fictional character Palantir uses when it shows prospective customers how its products work. This paragraph summarizes the information in Vance & Stone, *supra* note 129.

132. *Id.*

Miami; photos of his rental truck license plate from a tollbooth; phone records showing calls to Syria; and a map of his national and international movements.[133] Mouse clicks reveal more: Fikri has been wiring money to the people in Syria he has been calling; the Syrians, under investigation already, have been meeting daily for two weeks and have purchased plane tickets with Fikri's money; and a map traces the money flow from Cairo to Fikri in Miami, and from Fikri to the Syrians.[134] In light of the information, the Miami police arrest Fikri.[135]

Massive databases hold the information that Palantir analyzes. The Department of Homeland Security (DHS), for example, maintains "fusion centers" formed after 9/11 to aggregate and analyze massive amounts of data.[136] Information flows into government aggregation centers from government and private entities.[137] It is in fact "a two-way street. Banks, universities, hotels, defense companies like Boeing, and even Starbucks can be interpreted as 'critical infrastructure,' so fusion centers can share information with them and in some instances even allow private-sector representatives to be a part of investigations."[138]

---

133. *Id.*

134. *Id.*

135. *Id.*

136. *National Network of Fusion Centers Fact Sheet*, U.S. DEP'T HOMELAND SECURITY, http://www.dhs.gov/safeguard-and-secure-cyberspace (last updated Aug. 21, 2015). DHS maintains these centers in part because DHS has "the lead for the federal government for securing civilian government computer systems, and works with industry and state, local, tribal and territorial governments to secure critical infrastructure and information systems." *Safeguard and Secure Cyberspace*, U.S. DEP'T HOMELAND SECURITY, http://www.dhs.gov/safeguard-and-secure-cyberspace (last visited Oct. 16, 2015). The data is necessary "to make the most of the fast-growing volume of digital data . . . . [b]y improving our ability to extract knowledge and insights from large and complex collections of digital data, the initiative promises to help solve some the Nation's most pressing challenges." Press Release, Off. Sci. & Tech. Pol'y, Obama Administration Unveils "Big Data" Initiative: Announces $200 Million in New R&D Investments (Mar. 29, 2012), http://www.whitehouse.gov/sites/default/files/microsites/ostp/big_data_press_release.pdf. The Obama administration continues this commitment despite recent overtures on reevaluating the relationship between privacy and data collection. *See Remarks by the President on Review of Signals Intelligence*, THE WHITE HOUSE (Jan. 17, 2014, 11:15 AM), https://www.whitehouse.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence.

137. GILLIOM & MONAHAN, *supra* note 4, at 123.

138. *Id.*

Fusion centers are not the only government aggregation and distribution initiatives. The FBI's Next Generation Identification[139] and Integrated Automated Fingerprint Identification System (IAFIS) integrate biometric information across multiple databases providing "a national fingerprint and criminal history system that responds to requests 24 hours a day, 365 days a year . . . [and] provides automated fingerprint search capabilities, latent search capability, electronic image storage, and electronic exchange of fingerprints and responses."[140] IAFIS includes "[n]ot only fingerprints, but corresponding criminal histories; mug shots; scars and tattoo photos; physical characteristics like height, weight, and hair and eye color; and aliases" from federal and state law enforcement agencies and "criminal justice partners."[141] The system focuses on criminals, but it does include information on civilians, "mostly of individuals who have served or are serving in the U.S. military or have been or are employed by the federal government."[142]

3. The Public/Private Surveillance Partnership

The government's data collection and aggregation/distribution efforts are impressive, but they pale in comparison with the private sector. As Ronald Diebert notes,

> in a very real sense we no longer move about our lives as self-contained beings, but as nodes of information production in a dense network of digital relations involving other nodes of information production. All of the data about us as individuals in social network communities is owned, operated, managed, and manipulated by third parties beyond our control, and those third parties are, typically, private companies. In assessing the full spectrum of major social changes related to the information revolution, the entrusting of this unimaginably huge mass of civilian data in private sector hands ranks as perhaps the most important.[143]

Governmental access to this "unimaginably huge mass of civilian data" vastly increases the reach of what the

---

139. *Next Generation Identification (NGI)*, FED. BUREAU INVESTIGATION, https://www.fbi.gov/about-us/cjis/fingerprints_biometrics/ngi (last visited Oct. 16, 2015).

140. *Integrated Automated Fingerprint Identification System*, FED. BUREAU INVESTIGATION, http://www.fbi.gov/about-us/cjis/fingerprints_biometrics/iafis/iafis (last visited Oct. 16, 2015).

141. *Id.*

142. *Id.*

143. DEIBERT, *supra* note 4, at 63.

government knows about its citizens. This is what drives Schneier's "welcome to a world" worries: "Welcome to a world where all of this, and everything else that you do or is done on a computer, is saved, correlated, studied, passed around from company to company without your knowledge or consent; and where the government accesses it at will without a warrant."[144] It is an exaggeration to claim "the government accesses it at will without a warrant."[145] The government's access to the information is extensive nonetheless.

The government routinely purchases information from data aggregators such as Lexis/Nexis, Acxiom, Experian, and Datalogix.[146] In addition, it obtains information from voluntary government/private sector sharing programs,[147] statutes authorizing, or in some cases mandating, information transfers with only a subpoena or less.[148] In general, information flows

---

144. *The Internet Is a Surveillance State*, *supra* note 6.

145. *See infra* notes 147–150 and accompanying text (noting the voluntary nature of government-private sector sharing programs).

146. Sandra Fulton, *Senate Report Opens a Window Into Hidden World of Data Aggregators*, AM. CIVIL LIBERTIES UNION (Dec. 18, 2013, 3:51 PM), https://www.aclu.org/blog/technology-and-liberty/senate-report-opens-window-hidden-world-data-aggregators; *see also* JAY STANLEY, AM. CIVIL LIBERTIES UNION, THE SURVEILLANCE-INDUSTRIAL COMPLEX: HOW THE AMERICAN GOVERNMENT IS CONSCRIPTING BUSINESSES AND INDIVIDUALS IN THE CONSTRUCTION OF A SURVEILLANCE SOCIETY 25 (2004).

147. The Department of Homeland Security's Enhanced Cybersecurity Services is an example:

> (ECS) is a voluntary information sharing program that assists U.S.-based public and private entities [critical infrastructure owners and operators] as they improve the protection of their systems from unauthorized access, exploitation, or data exfiltration. DHS works with cybersecurity organizations from across the federal government to gain access to a broad range of sensitive and classified cyber threat information . . . .
>
> The ECS program does not involve government monitoring of private networks or communications . . . . However, when a CSP customer voluntarily agrees, the CSP may share limited and anonymized information with ECS.

Enhanced Cybersecurity Services, U.S. DEP'T HOMELAND SECURITY, http://www.dhs.gov/enhanced-cybersecurity-services (last visited Oct. 16, 2015).

148. *See* Reidenberg, *supra* note 4, at 589–90 (citing Erin Murphy, *The Politics of Privacy in the Criminal Justice System: Information Disclosure, the Fourth Amendment, and Statutory Law Enforcement Exemptions*, 111 MICH. L. REV. 485, 516–18 (2012) ("[A] plethora of statutory provisions permit law enforcement access to privately held data, . . . the typical mechanism is a judicial subpoena rather than a warrant, and . . . subpoenas while easy to obtain may be conditioned on prior notice or higher evidentiary standards."));

readily between government and business, a situation Schneier aptly labeled "the public-private surveillance partnership."[149] As he notes, "[g]overnments are happy to use the data corporations collect . . . . And corporations are happy to buy data from governments."[150]

B. USE

The government uses the information it has to discourage and prevent behavior of which it disapproves. Current critiques of governmental surveillance tend to focus on this fact. Their examples include journalists,[151] political dissenters,[152] lawyers representing political activists and dissenters,[153] politicians opposing the policies and goals of those with the power to order surveillance,[154] sustainable energy advocates,[155] environmentalists,[156] animal rights activists,[157] Afro-Americans,[158] Muslims,[159] labor unions,[160] people seeking health care,[161] welfare recipients,[162] parolees,[163] and a diverse collection of types of people the government regards as (possibly) undesirable.[164] Critiques of surveillance typically

---

see also Slobogin, *supra* note 6; Stephen W. Smith, *Gagged, Sealed & Delivered: Reforming ECPA's Secret Docket*, 6 HARV. L. POL'Y REV. 313 (2012); Glenn Greenwald & James Ball, *Revealed: The Secret Rules that Allows NSA to Use Data Without a Warrant*, GUARDIAN, Jun. 21, 2013, at 30.

149. *See* Bruce Schneier, *The Public-Private Surveillance Partnership*, SCHNEIER ON SECURITY (July 31, 2013), https://www.schneier.com/essay-436.html.

150. *The Internet Is a Surveillance State*, *supra* note 6.

151. BOGHOSIAN, *supra* note 4, at 173–86.

152. *Id.* at 107–12, 249–63.

153. *Id.* at 155–72.

154. *See generally* THEOHARIS, *supra* note 4.

155. BOGHOSIAN, *supra* note 4, at 35–50.

156. *Id.* at 57.

157. *Id.* at 140–42.

158. *Id.* at 76.

159. *Id.* at 84–86.

160. THEOHARIS, *supra* note 4, at 45–67.

161. *See generally* AMY L. FAIRCHILD ET AL., SEARCHING EYES: PRIVACY, THE STATE, AND DISEASE SURVEILLANCE IN AMERICA 1–29 (2007).

162. CHRISTIAN PARENTI, THE SOFT CAGE: SURVEILLANCE IN AMERICA FROM SLAVERY TO THE WAR ON TERROR 162–68 (2003).

163. *Id.* at 169–75.

164. *See, e.g.*, *id.* at 178 ("[P]olice in Wilmington, Delaware, began compiling a database—not of gangbangers or their associates—but of people who authorities believed might break the law sometime in the future. Within

claim that some or all of these uses are *illegitimate* in the sense that the government's goal is to discourage or prevent activities typically considered permissible in a democratic state.[165] The claim is not without merit, but its validity does not matter here. Our point is about *all* governmental use of surveillance-based information—legitimate and illegitimate alike. *All* of it can have a chilling effect that undermines the norm-enabled coordination necessary for privacy in public. We offer two examples, both of which we also discuss in the next section.

Greenwald and Snowden are the first example. Snowden first contacted Glen Greenwald by email using the pseudonym Cincinnatus.[166] Snowden's concern about governmental surveillance led him to insist on PGP encryption.[167] As Greenwald explains, "[t]he email began: 'The security of people's communications is very important to me,' and its stated purpose was to urge me to begin using PGP encryption so that 'Cincinnatus' could communicate things in which, he said, he was certain I would be interested."[168] Greenwald did not bother to respond.

> I frequently hear from all sorts of people offering me a "huge story," and it usually turns out to be nothing. And at any given moment I am usually working on more stories than I can handle. So I need something concrete to make me drop what I'm doing in order to pursue a new lead.[169]

Snowden's concern about government surveillance prevented effective communication.

---

two months special 'jump out squads' had begun files on over 200 people, almost all of whom were Black or Latino. Just to be perfectly clear: the subjects of the new database were not arrested for crimes or even considered suspects. Instead they were simply people—usually poor Black people—whom the cops had stopped, frisked, interrogated, photographed, and then opened a file because the subject had been found in so-called 'hot spots' known for violence and drug dealing.").

165. *See supra* note 4.

166. GREENWALD, *supra* note 4 at 7 ("[It was] a reference to Lucius Quinctius Cincinnatus, the Roman farmer who, in the fifth century BC, was appointed dictator of Rome to defend the city against attack. He is most remembered for what he did after vanquishing Rome's enemies: he immediately and voluntarily gave up political power and returned to farming life. Hailed as a 'model of civic virtue,' Cincinnatus has become a symbol of the use of political power in the public interest and the worth of limiting or even relinquishing individual power for the greater good.").

167. *Id.* at 8.

168. *Id.* at 7.

169. *Id.* at 9.

This may seem like an inapposite example for us to use. Our focus is on privacy in public, but Snowden's concern was about email eavesdropping.[170] Both norms and laws treat email content much like the content of sealed letters, a paradigm of privacy *by enclosure*.[171] To see the connection to privacy *in public*, consider how Greenwald and Snowden would have communicated if surveillance had not been a concern. Snowden would face the possibility that Greenwald would disclose his identity to the government, but that would not stop him from disclosing enough information to convince Greenwald that there was indeed a "huge story." He knew Greenwald's reputation as a politically active journalist, so he would have been certain that Greenwald would adhere to the journalist "protect your source" norm. Thus, privacy-in-public-creating coordination would have occurred. It initially did not because of Snowden's concern about surveillance. As Greenwald puts it,

> [we] found ourselves in a Catch-22. He was unwilling to tell me anything specific about what he had, or even who he was and where he worked, unless I installed encryption. But without the enticement of specifics, it was not a priority to respond to his request and take the time to install the program.[172]

He adds, "That's how close I came to blowing off one of the largest and most consequential national security leaks in US history."[173]

The second example is the generalization from the Greenwald/Snowden case to any journalist and whistleblower. Imagine they wish to disclose the perceived governmental wrongdoing in mainstream media. Doing so ensures widespread readership and a patina of legitimacy and truthfulness. Securing publication can be problematic, however. The problem is that "writers and editors for major publications and broadcast networks [engage in] a process of consultation with government, and of voluntary self-restraint, that is continual and intense."[174] As Greenwald notes, there are

---

170. *Id.* at 8.

171. On norms, see *supra* Section I, A. For a judicial treatment of email as similar to a sealed letter, see *U.S. v. Warshak*, 631 F.3d 266, 284 (6th Cir. 2010).

172. GREENWALD, *supra* note 4 at 10.

173. *Id.*

174. Allan M. Siegal, *Secrets About Secrets: The Backstage Conversations Between Press and Government* 3 (Joan Shorenstein Ctr. on the Press, Pol., & Pub. Pol'y, Working Paper No. 2007-2, 2007).

> unwritten protective rules that govern how the establishment media report on official secrets. According to these rules, which allow the government to control disclosures and minimize, even neuter, their impact, editors first go to officials and advise them what they intend to publish. National security officials then tell the editors all the ways in which national security will supposedly be damaged by the disclosures. A protracted negotiation takes place over what will and will not be published. At best, substantial delay results. Often, patently newsworthy information is suppressed.[175]

The New York Times reporters James Risen and Eric Lichtblau are a good example. In mid-2004, they were ready to publish a story exposing the NSA's warrantless eavesdropping, but the Bush Administration pressured the Times into delaying publication for fifteen months—until Bush was reelected.[176] And, then, the Times only ran the story because Risen was about to scoop the paper by publishing the story in his Pulitzer Prize winning book, *State of War: The Secret History of the CIA and the Bush Administration*.[177] Since the 2006 publication, he has

> been pursued by both the Bush and Obama administrations in a six-year leak investigation into that book, "State of War: The Secret History of the CIA and the Bush Administration." Risen now faces years in prison if he refuses to testify at the trial of a former CIA officer, Jeffrey Sterling, who is accused of giving him classified information about the agency's role in disrupting Iran's nuclear program.[178]

As *New Yorker* reporter Jane Mayer observed, "[i]t's a huge impediment to reporting, and so chilling isn't quite strong enough, it's more like freezing the whole process into a standstill."[179] Indeed, faced with threats of subpoenas from the Department of Justice, Lichtblau stopped writing about

---

175. GREENWALD, *supra* note 4 at 55; *see also* Siegal, *supra* note 174 *passim*; Margaret Sullivan, Editorial, *Lessons in a Surveillance Drama Redux*, N.Y. TIMES, Nov. 9, 2013, at SR12.

176. Byron Calame, *Eavesdropping and the Election: An Answer on the Question of Timing,* N.Y. TIMES, Aug. 13, 2006, at C10.

177. JAMES RISEN, STATE OF WAR: THE SECRET HISTORY OF THE CIA AND THE BUSH ADMINISTRATION (2006); Gabriel Sherman, *Why Times Ran Wiretap Story, Defying Bush*, N.Y. OBSERVER, Dec. 26, 2005, at 1.

178. *James Risen Prepared to "Pay Any Price" to Report on War on Terror Amid Crackdown on Whistleblowers*, DEMOCRACY NOW! (Oct. 14, 2014), http://www.democracynow.org/2014/10/14/james_risen_prepared_to_pay_any.

179. Molly Redden, *Is the 'Chilling Effect' Real?*, NEW REPUBLIC (May 15, 2013), http://www.newrepublic.com/article/113219/doj-seizure-ap-records-raises-question-chilling-effect-real.

national security at the end of the Bush Administration.[180] Risen continued (and continues) to write about national security,[181] and, while he was ultimately not called to testify at the Sterling trial,[182] he still describes the time as "the most stressful and traumatic time of my life."[183]

C. MERELY KNOWING

As worrisome as the journalist examples may be, most people are not journalists—or political dissenters, lawyers representing dissenters, or engaged in any activity that is likely to expose them to a serious risk of governmental reprisals based on surveillance information. Compare use with merely knowing. The government knows a great deal about everyone. Can the mere fact that government merely knows have a chilling effect independent of the concern that the government will use that information to your detriment? If so, the chilling effect of merely knowing has far greater potential reach than the chilling effect of use.

The answer to whether merely knowing can have a chilling effect is, "Yes, without question." What the government knows about you determines how you appear to the government, and controlling how you appear to the government is critical to adequate self-realization, as we noted earlier.[184]

A clear example is *First Unitarian Church of Los Angeles v. NSA*.[185] Twenty-four organizations, represented by the Electronic Frontier Foundation (EFF), filed the case alleging that bulk data collection under PATRIOT Act Section 215

---

180. *Id.* ("Lichtblau said that subpoena threats from the DOJ were 'the trigger' that caused him to quit writing national security stories in the closing days of the Bush administration.").

181. JAMES RISEN, PAY ANY PRICE: GREED, POWER, AND ENDLESS WAR (2014).

182. Matt Apuzzo, *C.I.A. Officer Guilty in Leak Tied to Reporter*, N.Y. TIMES, Jan. 27, 2015, at A1.

183. Sullivan, *supra* note 175.

184. *See supra* Section II, C.

185. Complaint, First Unitarian Church of Los Angeles v. National Security Agency, No. 13-cv-03287 (N.D. Cal. July 16, 2013); Aaron Mackey, *Update on* First Unitarian Church v. NSA*: EFF's First Amendment Challenge to NSA Spying*, ELEC. FRONTIER FOUND. (Sept. 18, 2015), https://www.eff.org/deeplinks/2015/09/update-eff-case-arguing-nsa-spying-violated-groups-first-amendment-rights.

violated their First Amendment right of association.[186] The EFF explains that

> The collection and analysis of telephone records give the government a broad window into our associations. The First Amendment protects against this because, as the Supreme Court has recognized, "it may induce members to withdraw from the association and dissuade others from joining it because of fear of exposure of their beliefs shown through their associations and of the consequences of their exposure."[187]

As the twenty-four declarations the plaintiffs filed show, "fear of exposure of their beliefs" has a chilling effect that is complementary to but independent of "fear . . . of the consequences of their exposure."[188] For example, Mathew Wood, Policy Director of Free Press,[189] claims that

> our members who wish to speak about the Associational Tracking Program [EFF's label for bulk data collection under Patriot Act Section 215] . . . have conveyed to me . . . their reservations and increased concern about discussing such topics in the knowledge that the . . . government is tracking their communications—and in the belief that speaking out against these programs could, perversely, result in additional scrutiny and monitoring of such members' communications with our organization, government officials, and our members' friends and family members.
>
> The Associational Tracking Program activities have thus harmed Free Press because we have experienced a decrease in telephone communications from members and constituents who had desired the fact of their communication to our organization and to their elected representatives either to remain secret or to remain free from such tracking and monitoring.[190]

The source of the chilling effect is the government's knowledge—its *merely* knowing, not its possible use of its knowledge to the detriment of the members of the association. Many are willing to take on the role of association member or

---

186. Mackey, *supra* note 185.

187. First Unitarian Church of Los Angeles v. NSA, ELEC. FRONTIER FOUND., https://www.eff.org/cases/first-unitarian-church-los-angeles-v-nsa (last visited Oct. 16, 2015) (quoting NAACP v. Alabama, 357 U.S. 449, 462–63 (1958)).

188. *See id*.

189. FREE PRESS, http://www.freepress.net/ (last visited Oct. 16, 2015).

190. Declaration of Matthew F. Wood for Free Press in Support of Plaintiffs' Motion for Partial Summary Judgment, First United Unitarian Church v. NSA, Case No. 313-cv-03287 JSW ¶¶ 4-5 (N.D. Cal. 2013), https://www.eff.org/document/all-plaintiffs-declarations [hereinafter Declaration of Matthew F. Wood].

supporter in confidence, but not in a way that puts them on the government radar as a member or supporter.

This makes good sense in light of our earlier discussion of self-realization. Governmental surveillance turns the two-party organization/individual relationship into a three-party organization/individual/government relationship. As in the Italian trattoria example, remaining in the role of "member or supporter unknown to the government" may be quite important to peoples' choices about how they wish to live their lives. You may be willing to enter the two-party relationship but not willing to enter the three-party one, with the additional complications and concerns it entails. Being on the government's radar as a member of the Free Press may not be consistent with other choices you have made about how to pursue your self-realization. Note in this regard one key difference with the Italian trattoria. You can walk away from the restaurant, but you cannot walk away from the government.

Similar concerns about roles and control over appearance arise in other areas as well. Journalists and their confidential sources is an example. The Obama Administration's unprecedented threats and prosecutions of journalists and their sources have heightened concern, not just about the government's use of information, but also about what it merely knows. For example, in *With Liberty to Monitor All: How Large-Scale US Surveillance Is Harming Journalism, Law, and American Democracy*, the ACLU reports that

> Journalists expressed concern that, rather than being treated as essential checks on government and partners in ensuring a healthy democratic debate, they now feel they may be viewed as suspect for doing their jobs. One prominent journalist summed up what many seemed to be feeling as follows: "I don't want the government to force me to act like a spy. I'm not a spy; I'm a journalist."[191]

The complaint is not about possible governmental reprisals. It is about being forced to change how you live your life as a journalist. It is a complaint about changed self-realization. This is not to say that journalist do not worry about reprisals. They

---

191. HUMAN RIGHTS WATCH & AM. CIVIL LIBERTIES UNION, WITH LIBERTY TO MONITOR ALL: HOW LARGE-SCALE US SURVEILLANCE IS HARMING JOURNALISM, LAW AND AMERICAN DEMOCRACY 4 (2014), https://www.aclu.org/sites/default/files/assets/dem14-withlibertytomonitorall-07282014.pdf.

do, as the earlier Risen/Lichtblau example shows, but those concerns combine with concerns about self-realization.

Considerably more empirical work is called for to document the chilling effect of the government's merely knowing. Our contribution is theoretical. It consists in the model we develop in the next section of when and how governmental merely knowing undermines privacy in public. Two concepts play a key role in that model: complicity and uncertainty.

D. COMPLICITY

The dictionary definition of complicity is "involvement in wrongdoing."[192] We use complicity in a narrower sense. You are *complicit in surveillance* when you knowingly convey information to a third party in ways that violate relevant role-appropriate norms. The first example is mainstream media's adherence to the "unwritten protective rules that govern how the establishment media report on official secrets."[193] Those rules can lead media companies to divulge information to the government in ways that are inconsistent with the journalist norm to conceal the identity of confidential sources—either because the journalist outright discloses the source (presumably under legal compulsion), or because the government obtains enough information to infer the source's identity.

Will the norm violation have a chilling effect? Yes, for two reasons. The first is the same as in the "merely knowing" discussion above. Complicity turns the two-party journalist/source relationship into a multi-party journalist/source/media/government relationship. A source willing to enter the two-party relationship may not be willing to enter the multi-party one. Entering that relationship can put them on the government's radar in ways that may not be consistent with choices they have made about how to pursue their self-realization.[194] The source's concern need not be just about the *use* of information in reprisal. The source may also be

---

192. *Complicity*, DICTIONARY.COM, http://dictionary.reference.com/browse/complicity (last visited Feb. 18, 2015).

193. GREENWALD, *supra* note 4, at 55 (according to those rules, "editors first go to officials and advise them what they intend to publish," and then "[n]ational security officials . . . tell editors all the ways in which national security will supposedly be damaged by disclosures").

194. *See* Declaration of Matthew F. Wood, *supra* note 190, at ¶¶ 4–5.

concerned about the government's merely knowing. He or she may not want to publicly play the role of a whistleblower even in the absence of governmental reprisals. That could entail a profound, and very much unwanted, change in the source's life.

The second reason complicity will have a chilling effect is that complicity is a betrayal. A person expected to adhere to an informational coordination norm violates that expectation. That not only destroys the present attempt to coordinate, it chills future attempts to the extent that people stop expecting others to conform to the norm. Compare committed adherents to an informational coordination norm. They might well continue to coordinate under the norm even in the face of governmental surveillance—either by evasive strategies, or by simply daring to continue under the government's eyes. Complicity eliminates these possibilities by turning a former compatriot into a government informant.

Educational surveillance is another good example. It is common.[195] Colleges, universities, and schools from K through 12 use surveillance software to monitor students and teachers.[196] Educational surveillance turns a two-party student/teacher relationship into a multi-party relationship among the student, the teacher, the school, and the government.[197] The software makes teachers complicit in surveillance. They transfer information to the school in ways

---

195. For an excellent review, see Alan Rubel & Kyle Jones, *Student Privacy in Learning Analytics: An Information Ethics Perspective*, 31 INFO. SOC'Y (forthcoming 2015). *See also Best School Administration Software,* CAPTERRA, http://www.capterra.com/school-administration-software/#infographic (last visited Oct. 16, 2015).

196. "[N]early seven out of ten institutions [of higher education] (69%) currently view analytics as a major priority, and the importance of analytics in higher education is growing exponentially." EDUCAUSE CTR. FOR ANALYSIS & RESEARCH, ECAR STUDY OF UNDERGRADUATE STUDENTS AND INFORMATION TECHNOLOGY, 2013, at 35 (2013), https://net.educause.edu/ir/library/pdf/ERS1302/ERS1302.pdf; *see also* CTR. FOR DIGITAL EDUC., BIG DATA AND ANALYTICS IN K-12 EDUCATION: THE TIME IS RIGHT (2013), http://www.hmhco.com/~/media/sites/home/teachers/files/hmh-cde_issue%20brief_dataanalytics.pdf.

197. The government has relatively ready access to information obtained through educational surveillance. *See Family Educational Rights and Privacy Act (FERPA)*, U.S. DEP'T OF EDUC. (2014), http://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html (last visited Oct. 16, 2015) (although the Family Educational Rights and Privacy Act limits government access to educational information for schools that receive government funds, significant exceptions permit government access).

that result in multiple violations of the student/teacher informational norm under which students and teachers limit their information exchanges so that, in each course, students will be evaluated primarily in light of their academic achievements in that course.[198]

Jenzabar is one widely used platform.[199] It claims to be "the only LMS [learning management system] solution that integrates completely with your administrative system, giving you seamless data exchange—and up-to-the-minute information."[200] Adding Concourse from Intellidemia makes it "easy to extract data from each syllabus and aggregate them into a single report . . . to determine if courses are meeting program and institutional outcomes."[201] Jenzabar Retention software

> aggregates each student's information from disparate academic and administrative systems across your campus to create comprehensive student profiles. The result is *a 360 degree view of each student*—from academic performance and extracurricular engagement to financial aid and demographic information—providing you with deep insights into potential risk factors and probabilities of success.[202]

Providing information to construct the "360 degree view" violates the student/teacher norm.[203]

The violation has a chilling effect. Studies of school surveillance suggest surveillance creates hyper-vigilance and distrust that limit the information sharing that would otherwise occur under the student-teacher norm.[204] One

---

198. For our discussion of this norm, see *supra* notes 61–62, 75 and accompanying text, and Warner & Sloan, *Self, Privacy, and Power*, *supra* note 7, at 65, 71, 78–79.

199. *User Experience Portal & Mobile*, JENZABAR, http://www.jenzabar.com/higher-ed-solutions/user-experience (last visited Oct 16, 2015).

200. *Learning Management System (LMS)*, JENZABAR, http://www.jenzabar.com/higher-ed-solutions/learning-management-system-lms (last visited Oct. 16, 2015).

201. *Concourse: Features*, INTELLIDEMIA, http://www.intellidemia.com/products/features/ (last visited Oct. 16, 2015).

202. *Jenzabar Retention: Student Successes Through to Completion*, JENZABAR (2013), http://www.jenzabar.com/sites/default/files/resource-downloads/Jenzabar_Retention_Brochure_web_2.pdf (emphasis added).

203. Warner & Sloan, *Self, Privacy, and Power*, *supra* note 7, at 65 ("[S]tudents and teachers . . . typically exchange only the information necessary to their interaction in those roles and voluntarily refrain from requesting, disclosing, or otherwise discovering more.").

204. EMMELINE TAYLOR, SURVEILLANCE SCHOOLS: SECURITY, DISCIPLINE AND CONTROL IN CONTEMPORARY EDUCATION 66–67 (2013); Andrew Hope,

explanation certainly is that students limit their disclosures because of concerns about *use*. They may fear the consequences of being categorized as, for example, uncooperative, troubled, antisocial, and so on. There are however—and this is the point we emphasize—two complementary explanations. The first is concern about merely knowing. Educational surveillance can make students appear to both the school and government in ways inconsistent with choices students have made about how to pursue their self-realization.[205] The second is betrayal. The informational norm requires that teachers not disclose certain information, and in blatant violation of the norm, they disclose it.

We conclude with the same two points we made when discussing merely knowing above. More empirical work is called for, and our contribution is a theoretical framework that may help guide such research. In developing that framework, we focus particularly on complicity.

Seductions of Risk, Social Control, and Resistance to School Surveillance, *in* SCHOOLS UNDER SURVEILLANCE: CULTURES OF CONTROL IN PUBLIC EDUCATION 230, 233–37 (Torin Monahan & Rodolfo D. Torres eds., 2010); *see, e.g.*, PARENTI, *supra* note 162; Craig Haney, *The Psychological Impact of Incarceration: Implications for Post-Prison Adjustment* 7–11 (U.S. Dep't of Health and Human Servs. & The Urban Inst., Working Paper, 2001), http://img2.timg.co.il/CommunaFiles/19852476.pdf; Stephen Parker & Rodney Fopp, *Mutual Obligation? Regulating by Supervision and Surveillance in Australian Income Support Policy*, 3 SURVEILLANCE SOC'Y 107, 115–20 (2005), http://www.surveillance-and-society.org/Articles3(1)/mutual.pdf. There are studies of the use of closed circuit television (CCTV), biometric identification, radio frequency identification devices (RFID), and full time police presence. The studies are consistent with the results of studies on the psychological impact of surveillance in other contexts. *See, e.g.*, PARENTI, *supra* note 162; Haney, *supra*; Parker & Fopp, *supra*.

205. The Privacy and Civil Liberties Oversight Board makes the same point about the bulk collection of telephone records:

> [T]he bulk collection of telephone records can be expected to have a chilling effect on the free exercise of speech and association, because individuals and groups . . . who for various reasons justifiably do not wish the government to know about their communications — must either forgo such activities, reduce their frequency, or take costly measures to hide them from government surveillance.

PRIVACY & CIVIL LIBERTIES OVERSIGHT BD., REPORT ON THE TELEPHONE RECORDS PROGRAM CONDUCTED UNDER SECTION 215 OF THE USA PATRIOT ACT AND ON THE OPERATIONS OF THE FOREIGN INTELLIGENCE SURVEILLANCE COURT 12 (2014), http://www.pclob.gov/Library/215-Report_on_the_Telephone_Records_Program.pdf.

E. UNCERTAINTY

Uncertainty plays a key role in undermining privacy in public. We explain what we mean by uncertainty here, and turn to its undermining role in the next section. To introduce the idea, note that governmental access to massive amounts of data raises two questions. *The knowledge question*: "What is the probability that the government knows X about me?" *The use question*: "Given that the government knows X, what is the probability that it will use that knowledge to my detriment?" So far, we have tacitly assumed that individuals can answer both questions by specifying a probability. This is not to say that people can answer with a precise number, like seventy percent. Everyday thought about probabilities typically proceeds in terms of a range from extremely likely to extremely unlikely. People "specify a probability" when they demarcate a region in that range in a way that is sufficiently clear and definite for practical purposes. We will call cases in which people are able to specify a probability *specific probability cases*. Sometimes people cannot specify a probability in response to a knowledge or use question. The answer to the request for a specific probability in such cases is, "I have no idea what the specific probability is." We will describe these cases as instances of *uncertainty*.[206]

Uncertainty can arise with regard to both the knowledge and use questions. We focus on the former but, for completeness, begin with uncertainty about use. The subpoena threat Lichtblau faced is an example.[207] Imagine him asking, "Given what the government knows about me, how likely is the government to issue a subpoena?" It can be quite difficult to answer with a specific probability. "[R]eporters can lawfully be compelled to reveal the identities of those who have disclosed classified information to them," but "the Justice Department's internal guidelines caution prosecutors against compelling the disclosure of the identity of a reporter's sources."[208] In general,

---

206. This technical use of "uncertainty" is standard in economics. *See* KEN BINMORE, RATIONAL DECISIONS 35 (2009) (providing the examples of playing roulette in a casino as an event where probabilities can be assigned, and betting on horses in a race as an event with "uncertainty" where it comparably does not "make sense to attribute a probability to such a one-off occurrence"); OSTROM, *supra* note 72, at 49.

207. *See* Redden, *supra* note 179.

208. SAGAR, *supra* note 80, at 106.

the government's willingness to use information to discourage or prevent behavior depends on government policy and the immense variety of factors that affect its implementation.[209]

Uncertainty about what the government knows has two primary sources: information asymmetry, and the mosaic effect.

Information asymmetry. As the information technology expert Alessandro Acquisti notes, "[a]dvancements in information technology have made the collection and usage of personal data often invisible. As a result, individuals rarely have clear knowledge of what information other people, firms, and governments have about them or how that information is used and with what consequences."[210] A good illustration (which happens to involve complicity) is a whistleblower whose goal is to disclose perceived governmental wrongdoing in mainstream media while maintaining secrecy about his or her identity. The media company's contact with the government *may or may not* lead to demands that it reveal the identity of the source, and the media company *may or may not* comply.[211] As we noted earlier, journalists "can lawfully be compelled to reveal the identities of those who have disclosed classified information to them," but "the Justice Department's internal guidelines caution prosecutors against compelling the disclosure of the identity of a reporter's sources."[212] Earlier, this point supported a point about use: the claim that a journalist may not be able to specify the probability with which the government will compel them to reveal their source. This time it supports a point about knowing: a whistleblower may not be able to specify the probability that the government will learn his or her identity.

The mosaic effect. Combining information into large collections can reveal things that no significantly smaller subset does.[213] That effect is the mosaic effect. Thus, even if,

---

209. *See generally id.* at 17, 30–49 (discussing use of secrecy to protect the national interest by presidents from the nineteenth century to present day).

210. Alessandro Acquisti, Laura Brandimarte & George Loewenstein, *Privacy and Human Behavior in the Age of Information*, 347 SCIENCE 509, 509 (2015).

211. *See* Alan E. Garfield, *Promises of Silence: Contract Law and Freedom of Speech*, 83 Cornell L. Rev. 261, 273–74 (1998).

212. SAGAR, *supra* note 80, at 106.

213. B. Rose Huber, *'Mosaic Effect' Paints Vivid Pictures of Tech Users' Lives, Felten Tells Privacy Board*, WOODROW WILSON SCH. PUB. & INT'L AFF.

implausibly, you know everything the government knows about you, you may not know what they will infer from the aggregation of what they know. To take a simple example involving a very small amount of data, suppose that you travel frequently to Eastern Europe to teach legal education programs. Combining information about your ticket purchases with your online bio easily leads to that conclusion. But what is the specific probability that the government has drawn that conclusion? Or, some less desirable conclusion? The answer can easily be, "I have no idea."

IV. HOW SURVEILLANCE UNDERMINES COORDINATION

Surveillance threatens norm-enabled coordination through concern about the use of information and through concern about loss of control over appearance. We use a well-known part of game theory, the Assurance Game, to show when and why.

A. THE ASSURANCE GAME

The Assurance Game gets its name from the way in which its outcome depends on what each player thinks the other will do.[214] Suppose, for example, that Victor and Victoria are

---

(Nov. 20, 2014), http://wws.princeton.edu/news-and-events/news/item/mosaic-effect-paints-vivid-pictures-tech-users-lives-felten-tells-privacy; *see also* David E. Pozen, Note, *The Mosaic Theory, National Security, and the Freedom of Information Act*, 115 YALE L.J. 628 (2005) (chronicling the dramatic increase in the Bush Administration's use of mosaic theory to deny information requests after 9/11, and the evolving jurisprudence on the meaning and foundation of mosaic arguments); Daniel J. Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 STAN. L. REV. 1393 (2001) (highlighting the compounding loss of privacy that results from combining databases of information).

214. The game goes by a variety of names besides Assurance Game. Others are Trust Dilemma, Coordination Game, and Stag Hunt. WILLIAM POUNDSTONE, PRISONER'S DILEMMA 219 (1992). "Stag Hunt" is perhaps the most used name. It harks back to Rousseau's description of the stag hunt dilemma (the translation uses "deer" instead of "stag"): "Was a deer to be taken? Every one saw that to succeed he must faithfully stand to his post; but suppose a hare to have slipped by within reach of any one of them, it is not to be doubted but he pursued it without scruple." JEAN-JACQUES ROUSSEAU, A DISCOURSE UPON THE ORIGIN AND THE FOUNDATION OF THE INEQUALITY AMONG MANKIND 32 (Cosimo 2008) (1755). We use "Assurance Game" to emphasize the role of knowledge—or lack of it—in determining what the players do. For a discussion of the importance of the Assurance Game to

discussing by cell phone whether to meet at the opera later in the evening or whether each will stay home alone. Before they decide, their phone batteries run out, and they have no other way to communicate. They both have, and know they both have, the following preferences in the following order. (1) Attend the opera together. (2) Stay home alone when the other does too. (3) Stay home alone when the other goes to the opera. Neither wants to pass up meeting at the opera. (4) Go to the opera when the other does not.

The Assurance Game consists of two players with similar preferences.[215] But exactly what preferences? They do not always involve operas and homes. To generalize, think of going to the opera as *cooperating* in the attempt to meet at the opera, and staying home as *defecting* from the coordination needed to meet at the opera. For appropriate specifications of cooperation and defection, an Assurance Game consists of two parties with these preferences: (1) cooperate when the other cooperates; (2) defect when the other defects; (3) defect when the other cooperates; (4) cooperate when the other defects.

What will Victor and Victoria do? Focus on Victoria (essentially the same remarks hold for Victor). What she will do depends in part on how much she values her options relative to each other. We will describe the relative values using a scale of 10 to -10. This is the beginning of a small bit of mathematical precision that is a useful and harmless idealization. It is useful because the idealization allows us to derive results easily and clearly. It is harmless because the results remain valid for the un-idealized reality. Suppose, then, that Victoria rates meeting

---

analyzing social coordination, see BRIAN SKYRMS, THE STAG HUNT AND THE EVOLUTION OF SOCIAL STRUCTURE 1–14 (2004).

215. In addition, the parties are unable to communicate, and each chooses without observing or otherwise learning about the choice of the other. These assumptions, and the joint knowledge of one another's preferences, are classic assumptions of game theory. *See generally, e.g.*, KEVIN LEYTON-BROWN & YOAV SHOHAM, ESSENTIALS OF GAME THEORY: A CONCISE, MULTIDISCIPLINARY INTRODUCTION (2008); MARTIN J. OSBORNE & ARIEL RUBINSTEIN, A COURSE IN GAME THEORY (1994). The game theory literature is not completely consistent on terminology. Some definitions allow for variations such as both players being indifferent between outcomes (2) and (3), and some make distinctions between "Stag Hunt" and "Assurance Game" based on this sort of difference. The crucial point is that both outcomes where the two players do the same thing form Nash equilibria, with one having a higher payoff than the other. *See, e.g.*, SAMUEL BOWLES, MICROECONOMICS: BEHAVIOR, INSTITUTIONS, AND EVOLUTION 43 (2003).

Victor at the opera at 5. On the other hand, she regards that going to the opera when Victor does not as a disaster, so she rates that –10. Staying home alone when Victor also does is 3; while staying home when Victor goes to the opera is 1. The 3 versus 1 difference represents the value Victoria places on coordinating with Victor. Given these valuations, should Victoria go to the opera or stay home?[216] It is important to distinguish between the specific probability and uncertainty cases.

Specific probability cases. Assume Victoria answers the question, "How likely is it that Victor will go to the opera?" with "80%." Victoria's answer means she can infer the probability of Victor staying home alone. Since Victor will either go to the opera or stay home, the probability of his staying home is the same as the probability of his not going to the opera: 100% – 80% = 20%. With these probabilities, she calculates the expected value of her going to the opera and of her staying home alone: respectively, 2.0 and 1.4.[217] So, insofar as she is rational, Victoria will go to the opera. Indeed, Victoria arrives at a more general conclusion: to go to the opera only if she believes the probability of Victor going is 76% or greater. She arrives at that conclusion by asking, "When do going to the opera and staying home have the *same* expected value?" The answer is, when the probability of Victor going to the opera is

---

216. If Victor and Victoria played out this scenario on a regular basis, then in game theory terminology we would have a repeated game rather than a one-shot game. For repeated games, game theory predicts that the players will settle into one of the two Nash Equilibria, either both going to the opera or both staying home, and stay in that equilibria. *See, e.g.*, EVELYN C. FINK, SCOTT GATES & BRIAN D. HUMES, GAME THEORY TOPICS: INCOMPLETE INFORMATION, REPEATED GAMES, AND N-PLAYER GAMES 32–47 (1998). For our one-shot case, the player's dilemma is whether to go to the opera, intuitively aiming for the payoff-dominant best possible outcome of going to the opera together, or to stay home, avoiding the risk of going to the opera when the other stays home. For the seminal technical treatment of this issue see John C. Harsanyi, *A New Theory of Equilibrium Selection for Games with Complete Information*, 8 GAMES ECON. BEHAV. 91, 91–122 (1995). In the main body of this article we try to illuminate some of the general ideas.

217. Going to the opera has two outcomes: meeting Victor, and not meeting Victor. Its expected value is the sum of the expected values of those two options: (0.8 x 5) + (0.2 x -10) = 2.0. Staying home likewise has two options: staying home when Victor does, and staying home when he does not, so the expected value of staying home is (0.2 x 3) + (0.8 x 1) = 1.4.

76%.[218] Below 76% staying home has the better expected value, so Victoria should only go to the opera if the probability of Victor going is at least 76%.

In the un-idealized reality, Victoria does essentially the same thing. She takes her rough estimates of probability and combines it with a typically non-quantitative understanding of how much she values the various options to make the best compromise she can between how much she values the options and the likelihood of realizing what she values by the actions open to her.

Uncertainty cases. Suppose Victoria answers, "What is the specific probability that Victor will go to the opera?" with "I have no idea." Imagine that she and Victor are new acquaintances and have little knowledge of each other's personal characteristics. She knows that there is some chance that Victor will go to the opera and some chance that he will decide to do something else, but she does not know, nor does she even have grounds for an educated guess about, what those probabilities are. She assumes that the distribution of opera-attending probabilities over people in Victor's situation exhibits more or less the bell-shaped curve of a standard distribution with a peak somewhere in the broad vicinity of probability 50%.[219]

It may seem that Victoria's uncertainty makes the expected value calculations we used earlier irrelevant. Not quite. She knows a crucial fact: she should only go to the opera if the probability of Victor going is above 76%. This makes going to the opera a risky choice. It does, that is, when combined with her assumption of a standard distribution of opera-attending probabilities over people in Victor's situation. Then, as far as Victoria knows, chances are the probability of Victor attending the opera is below 76%, so she is likely to end up at the opera alone if she goes. Her best choice is to stay home.

---

218. For any probability p, the expected value of going to the opera is (p x 5) + ((1 – p) x -10), and the expected value of staying home is ((1 – p) x 3) + (p x 1), so Victoria solves this equation to find the value of p: (p x 5) + ((1 – p) x -10) = ((1 – p) x 3) + (p x 1). The value of p is $13/17 \approx 0.76$.

219. To be more precise, we should say, "50% or lower." As the argument in the next paragraph shows, the father away from higher probability cases Victoria believes the peak of the curve to be, the stronger the argument that she will not go to the opera.

The Assurance Game model offers a way to explain when and why government surveillance undermines norm-governed coordination that creates privacy in public. We turn to that explanation now. We begin with the specific probability cases and then turn to uncertainty and complicity.

B. SPECIFIC PROBABILITIES

We discuss two examples. The first involves use and the second merely knowing. Greenwald and Snowden's initial attempts to communicate provide the first example. The first point to note is that they were involved in an Assurance Game. We describe the preferences using the "cooperate" and "defect" terms. "Cooperate" means collaborating with each other to expose the NSA. For Greenwald to cooperate is for him to seek to secure publication in mainstream media. For Snowden, it includes providing information sufficient to expose the NSA. "Defect" means not cooperating—for example, because the NSA prevented it, or because, for Snowden, he did not really have the requisite information, or because, for Greenwald, he could not convince editors to publish the stories. Given this understanding, their preferences were as follows: (1) Cooperate when the other cooperates. This is what both clearly want most.[220] (2) Defect when the other defects. Neither wants to waste time and take risks attempting to cooperate if the other is not going to cooperate. (3) Defect when the other cooperates.

---

220. Greenwald had written for "the past seven years . . . almost on a daily basis about the dangerous trends in US state secrecy, radical executive power theories, detention and surveillance abuses, militarism, and the assault on civil liberties." GREENWALD, *supra* note 4, at 14. Snowden explained his motivation this way:

> I understand that I will be made to suffer for my actions, and that the return of this information to the public marks my end. I will be satisfied if the federation of secret law, unequal pardon, and irresistible executive powers that rule the world that I love are revealed for even an instant.

Id. at 32. Snowden knew and respected Greenwald's reputation as a crusader who would take risks and resist the pressure to censor or suppress publication. *Id.* at 53 ("On several occasions, Snowden explained that he had wanted Laura and me [Greenwald] to be involved in the stories from the start because he knew we would report them aggressively and not be susceptible to government threats. He frequently referred to the *New York Times* and other major media outlets that had held up big stories at the government's request. But while he wanted aggressive reporting, he also wanted meticulous journalists to take as long as necessary to ensure that the facts of the story were unassailable and that all of the articles had been thoroughly vetted.").

Neither wants to pass up a chance to expose the NSA when it is possible to do so. (4) Cooperate when the other defects. Cooperating when the other defects means wasting time and pointlessly running the risk of governmental reprisals.

If surveillance had not been a concern, they would have easily both cooperated since Snowden would have revealed enough to remove Greenwald's conviction that he was just another person offering him a "huge story" that would turn out "to be nothing."[221] Snowden's concern about surveillance prevented that. He was certain that the government would detect unencrypted communication and intervene to prevent his exposing the NSA.[222] Cooperating meant installing encryption software, and Greenwald was unwilling.[223] His unwillingness is exactly what the Assurance Game model predicts.

It does so predict, that is, given plausible assumptions about how Greenwald valued the various options. There is need to argue that the following values "really are Greenwald's." A fictional Greenwald makes as good an example as the real one. We use a 10 to -10 scale again: (1) Mutual cooperation rates 10. Exposing the NSA was extremely important to Greenwald. (2) Greenwald did not want to waste time pursuing worthless leads. So, we assign a rating of 3 to defecting when Snowden defects. (3) Greenwald would hate to miss the opportunity to expose the NSA. Thus, -5 is a reasonable rating for defecting when Snowden cooperates. (4) Cooperating when Snowden defects means wasting time and running pointless risks of reprisals. So, rate it -10. These numbers exactly parallel Victoria's (we picked the numbers with this in mind), so it follows that Greenwald will cooperate only if he thinks the probability of Snowden's doing so is at least 76%; but, he did not think the probability was anywhere in that range. He thought it highly likely Snowden would "defect" by not really having documents that would expose the NSA.

To illustrate the effect of governmental merely knowing, consider any journalist and whistleblowing confidential source. We give "cooperate" and "defect" somewhat more general meanings. For the journalist, to cooperate is to seek publication

---

221. *Id.* at 9.
222. *Id.* at 9–10.
223. *Id.*

while maintaining secrecy of the source's identity; and, to defect is to fail to obtain publication or to fail to maintain secrecy. For the source, to cooperate is to provide documents that adequately document governmental wrongdoing; and, to defect is not to do so. The journalist and the source share the following Assurance Game preferences: (1) Cooperate when the other cooperates. Both want most to expose governmental wrongdoing. (2) Defect when the other defects. Neither wants wasted effort. (3) Defect when the other collaborates. Neither wants to pass up the opportunity to expose wrongdoing. (4) Cooperate when the other defects. Neither wants to run the risks of cooperation for no gain.

Governmental merely knowing can lead the source to defect even when the journalist cooperates. Governmental knowledge comes from covert surveillance and from "unwritten protective rules that govern how the establishment media report on official secrets."[224] Those rules ensure that a "protracted negotiation takes place over what will and will not be published."[225] Imagine a source who is willing to supply evidence of wrongdoing only if his or her identity can remain secret. The source's objection is not, or not only, that the government will use the information to the source's detriment. The objection is that the source does not want to appear to the government and the public as a whistleblower. That is inconsistent with the path of self-realization the source has chosen and wishes to continue. The source would have this objection even if disclosing the information had no other adverse consequences.

The source has two ways to preserve the secrecy of his or her identity. One way is to rely on the journalist's coordination (recall we defined cooperation to include maintaining secrecy); the other is to defect and so avoid interactions that would put the source's identity at risk of disclosure. When will the source defect to preserve secrecy? That depends of course, on how the source values the relevant options. Suppose, as is plausible, that they parallel the Greenwald/Victoria values. Thus: (1) Cooperate when the journalist cooperates: 10. (2) Defect when the journalist defects: 3. (3) Defect when the journalist cooperates: -5. (4) Cooperate when the journalist defects: -10. In

224. *Id.* at 55.
225. *Id.*

this case, the source will defect unless he or she believes the probability that the journalist will cooperate (and thus maintain secrecy) is fairly high (0.76). The Bush and Obama administrations' readiness to investigate and prosecute journalists and their confidential sources may well have convinced some sources that secrecy was much less likely than that. As *The New York Times* journalist Philip Shenon remarked, after the Bush Administration seized his phone records, "My goodness, if I were one of my sources, I would never talk to me again, even about stories that really would have been a public service."[226]

Journalist/source is just one of a vast number of relationships in which people exchange information under the protective shield of informational norms. Massive governmental data collection means the government may know a great deal about those relationships. When will people react like the source in the example above and "defect" from relationships by abandoning them or by continuing them while withholding information that they would have readily conveyed in the absence of governmental surveillance? They will if, like the source, they see a sufficiently large downside in the government's knowing certain information and think the probability sufficiently high that the government knows it. Will that happen? Uncertainty makes it more likely.

1. The Significance of Uncertainty

In the specific probability cases, people defect because they assign a specific probability to the government's using or knowing certain information. We focus on the knowledge cases. Information asymmetry and the mosaic effect can make it difficult for people to assign specific probabilities to whether the government knows some fact about them.[227] So, if the assignment of a specific probability were required for defection, massive governmental knowing would lead to defection only in the relatively limited cases in which people did assign specific probabilities.

In fact, uncertainty easily leads to defection. Suppose the source in the previous example is uncertain about whether the

---

226. Redden, *supra* note 179; *see also* Charles Lane, *N.Y. Times Must Surrender Reporters' Phone Data*, WASH. POST, Aug. 2, 2006, at A16.

227. *See* Huber, *supra* note 213.

government will learn his or her identity. Will the source defect? Use the same valuation of alternatives as before. Then the calculation is the same as in the Victor/Victoria opera example: the source will defect unless he or she believes the probability of the journalist's cooperating is at least 76%. But the source will believe the probability is below that and defect—assuming the source believes the distribution of governmental-knowledge probabilities takes more or less the bell-shaped curve of a standard distribution.

What does this mean for the ubiquitous surveillance of everyday life? Does it mean that massive governmental knowledge about everyone threatens massive defection? The right response is to ask, "defection from what?" We have defined "cooperate" and "defection" case by case for particular Assurance Games. Is there some type of Assurance Game everyone plays from which everyone might defect? There is. People play Assurance Games with respect to informational coordination norms that facilitate privacy in public. Pick any such norm—the student/teacher norm or the journalist/source norm, for example. "Cooperate" means conforming to the norm. "Defect" means not conforming. The parties interacting under such norms have the following Assurance Game preferences: (1) Cooperate when the other cooperates. This is most preferred because the parties have internalized the norm and value the privacy in public it creates and the self-realization it facilitates. (2) Defect when the other party defects. The attempt to cooperate is pointless when the other party does not cooperate. (3) Defect when the other party cooperates. Defecting in this case throws away an opportunity to realize the most preferred option of mutual coordination. (4) Cooperate when the other defects. Cooperation in this case wastes effort and pointlessly assumes whatever risks are attendant on coordination when the other defects.

At present, in a wide range of cases, people realize the cooperate/cooperate alternative and, thereby, create norm-based privacy in public. So surveillance, although pervasive, has not greatly disrupted norm-based coordination. Is there reason to think this will change? Complicity is one major reason.

2. The Significance of Complicity

Massive governmental knowing creates massive complicity. Contemporary surveillance turns individuals and institutions into informants on others. Individuals become informants on others because the data trails they leave do not reveal information just about *them*. They reveal the relationships with others woven into the pattern of their lives. Indeed, under our definition of complicity telephoning a friend can make you complicit in surveillance provided you are aware of the Snowden revelations about governmental data collection. The journalist/source and educational surveillance examples suggest widespread complicity will have a widespread undermining effect on coordination under informational norms. But it would be a mistake to conclude that this will happen across the board. Complicity has an undermining effect in the journalist/source and educational surveillance examples when sources and students assign a large disvalue to governmental merely knowing. The following analogy suggests that parties to norms may not always assign such a large disvalue.

Suppose Bob confides in Alice that he finds Carol gorgeous and cannot stop thinking about her, and Alice tells both Doug and Carol. Bob does not object to his best friend Doug knowing, but he assigns a large disvalue to Carol knowing. Her knowing deprives him of control over an aspect of the way he appears to her, and his control over his appearance in that regard is particularly important to him. His concern is not that she will use the information to harm him; he just did not want to appear to her in the role of someone obsessed with her beauty. So, are peoples' disvaluing of governmental knowledge more like Bob's reaction to Doug or to Carol? The answer is almost certainly neither. It is reasonable to expect the effect on coordination to spread across a spectrum from "extreme disvalue" to "minimal disvalue."

The future distribution of cases across this spectrum plays a key role in the future of surveillance. The distribution depends on the combined effect of use, merely knowing, and especially complicity. Will the betrayal of trust involved in complicity eventually lead people to assign a large disvalue to government surveillance?

V. THE FUTURE

As Niels Bohr and Yogi Berra both are reputed to have observed, "prediction is very difficult, especially about the future."[228] Accordingly, we outline three possible future scenarios and offer them, not as predictions, but as reference points to guide future choices.

A. THE STASI AS A REFERENCE POINT

The history of the Stasi makes current surveillance practices stand out in sharp relief. Four features characterized the Stasi's surveillance practices.

First, massive knowing: As we noted earlier, the Stasi engaged in massive data collection and hence knew a great deal about East German citizens.[229]

Second, complicity: Informants "spied on friends, workmates, neighbors and family members. Husbands spied on wives."[230] Even if the people with whom you interacted were not Stasi informants, the 1 in 50 distribution of informants[231] made it likely that friends, acquaintances, and acquaintances of your friends would be. "Relations between people were conditioned by the fact that one or other of you could be one of *them* [the Stasi]. Everyone suspected everyone else, and the mistrust this bred was the foundation of social existence."[232]

Third, pervasive repressive use: The Stasi translated its massive merely knowing into pervasive repressive use:

> At its heart, the Stasi was an organization that monitored society for those who . . . "thought differently." Stasi officers worked tirelessly to insure that a disruption to the socialist order—be it anti-state graffiti, the establishment of groups that did not conform to the SED's world-view, defections, or whatever form it might take—did not occur.[233]

---

228. *Yogi Berra Quotes*, FAMOUS QUOTES & QUOTATIONS, http://www.famous-quotes-and-quotations.com/yogi-berra-quotes.html (last visited Oct. 16, 2015); Quote Details: Niels Bohr, QUOTATIONS PAGE, http://www.quotationspage.com/quote/26159.html (last visited Oct. 16, 2015).

229. *See supra* notes 110–114 and accompanying text.

230. HARDING, *supra* note 2, at 254.

231. BRUCE, *supra* note 1, at 10 & 190 n.45.

232. ANNA FUNDER, STASILAND: STORIES FROM BEHIND THE BERLIN WALL 28 (2011).

233. BRUCE, *supra* note 1, at 140.

As the novelist Anna Funder notes in her study of the Stasi, it "arrested, imprisoned and interrogated anyone it chose."[234] She adds that "[m]any of the punishments were simply for lack of belief, or even suspected lack of belief. Disloyalty was calibrated in the minutest of signs: the antenna turned to receive western television, the red flag not hung out on May Day."[235]

Fourth, curtailed self-realization: Merely knowing, complicity, and repressive use severely curtailed possibilities for self-realization. As Gary Bruce puts it in his study of the Stasi,

> One does not detect from East Germans' reflections on their past that they were gripped by a paralyzing fear, in the psychological sense of the word—although one interview subject did say she "was always afraid"—but rather a deep resignation that one was not the master of one's own destiny, that to run afoul of the Stasi, even unintentionally, was to sacrifice power over one's life and the life opportunities of family members.[236]

The United States certainly outdoes the Stasi in the amount it knows and, perhaps, even in the extent of citizen complicity.[237] In this way, the United States has traveled down the road that leads to the Stasi. But it is far from Stasi-like surveillance. It differs—only, but critically—in being far more restrained in its use of information to discourage and prevent behavior the government finds undesirable. This is less reassuring than it may seem, however. There is a "tendency of

---

234. FUNDER, *supra* note 232, at 59.

235. *Id.* at 157.

236. BRUCE, *supra* note 1, at 158 (footnotes omitted).

237. Everyone with any online presence is unknowingly complicit in the transfer of information about others to private businesses and hence to the government through the public/private surveillance partnership. In that sense, complicity in surveillance greatly surpasses the Stasi's 1 in 50 informant ratio. Knowing complicity may do so as well. Post-Snowden, knowledge of government surveillance is widespread. According to a 2013 PEW survey, 50% of Americans answered "a lot" to: "How much, if anything, have you heard about the government collecting information about telephone calls, e-mails and other online communications as part of efforts to monitor terrorist activity?" Another 37% answered "a little." *PEW Research Center for the People & the Press July 2013 Political Survey*, PEW RES. CTR. FOR PEOPLE & THE PRESS (2013), http://www.people-press.org/files/legacy-questionnaires/7-26-13 NSA Topline for Release.pdf. Totaling the percentages yields 87% with some knowledge of government surveillance and hence, possibly, some knowledge of their own complicity. The extent of actual knowledge of complicity is unclear, and, as we argued in Section IV, D, the undermining effect of knowing complicity is unclear at present.

surveillance systems to spread. It simply lies in the interests of both government and private surveillance operations to expand—to cover more people and more of the lives of the people they cover."[238]

B. THREE POSSIBLE WORLDS

So what does the future hold?

1. A Stasi-Like World

Imagine the "tendency of surveillance systems to spread" leads the government to greatly expand the range of behavior it uses surveillance to prevent or discourage. Against that background, fear of reprisals, concern about merely knowing, uncertainty, and complicity combine to undermine norm-based coordination. Adequate privacy in public disappears and rich possibilities for self-realization vanish along with it.

Many may react with, "It can't happen here." The comments of a German philologist who witnessed the rise of the Nazis are a reminder that it could.

> What happened here was the gradual habituation of the people, little by little, to being governed by surprise; to receiving decisions deliberated in secret; to believing that the situation was so complicated that the government had to act on information which the people could not understand, or so dangerous that, even if people could understand it, it could not be released because of national security . . . .
>
> This separation of government from the people, this widening of the gap, took place so gradually and so insensibly, each step disguised (perhaps not even intentionally) as a temporary emergency measure or associated with true patriotic allegiance or with real social purposes. And all the crises and reforms (real reforms, too) so occupied the people that they did not see the slow motion underneath, of the whole process of government growing remoter and remoter . . . .
>
> . . . .
>
> . . . Each step was so small, so inconsequential, so well explained or, on occasion, 'regretted,' that, unless one were detached from the whole process from the beginning, unless one understood what the whole thing was in principle, what all these 'little measures' that no 'patriotic German' could resent must some day lead to, one no more saw it developing from day to day than a farmer in his field sees the corn growing . . . .
>
> . . . .

238. RULE, *supra* note 8, at 151.

> . . . Believe me, this is true. Each act, each occasion, is worse than the last, but only a little worse. You wait for the next and the next. You wait for one great shocking occasion, thinking that others, when such a shock comes, will join with you in resisting somehow.
>
> . . . .
>
> . . . Suddenly it all comes down, all at once. You see what you are, what you have done, or, more accurately, what you haven't done (for that was all that was required of most of us: that we do nothing) . . . . You remember everything now, and your heart breaks. Too late. You are compromised beyond repair.[239]

This is—we hope—an unlikely path. We think the second scenario more likely.

2. The "Pose No Challenge" Bargain

Governmental use of information to control behavior expands but stops far short of Stasi-like levels. People become accustomed to massive governmental merely knowing. They also become used to increasing individual and organizational complicity and do not assign a large disvalue to the transfer of information about norm-governed transactions to the government. Accepting massive complicity means accepting the government as an observer in norm-governed transactions. The effect is what numerous studies confirm: people increase their conformity to the standards they attribute to the watchers. Life becomes as Solzhenitsyn describes it in *Cancer Ward*:

> As every man goes through life he fills in a number of forms for the record, each containing a number of questions . . . . There are thus hundreds of little threads radiating from every man, millions of threads in all. If these threads were suddenly to become visible, the whole sky would look like a spider's web, and if they materialized as rubber bands, buses, trams and even people would all lose the ability to move, and the wind would be unable to carry torn-up newspapers or autumn leaves along the streets of the city. They are not visible, they are not material, but every man is constantly aware of their existence . . . .
>
> Each man, permanently aware of his own invisible threads, naturally develops a respect for the people who manipulate the threads.[240]

The ultimate result is a world in which an

> implicit [unacceptable] bargain . . . is offered to citizens: pose no challenge and you have nothing to worry about. Mind your own

---

239. MILTON MAYER, THEY THOUGHT THEY WERE FREE: THE GERMANS, 1933–45, at 166–72 (2d ed. 1966).

240. ALEKSANDR SOLZHENITSYN, CANCER WARD 208–09 (Nicholas Bethell & David Burg trans., Vintage 2003) (1968).

> business, and support or at least tolerate what we do, and you'll be fine. Put differently, you must refrain from provoking the authority that wields surveillance powers if you wish to be deemed free of wrongdoing. This is a deal that invites passivity, obedience, and conformity. The safest course, the way to ensure being "left alone," is to remain quiet, unthreatening, and compliant.[241]

It would be better if self-realization is not curtailed in ways that invite "passivity, obedience, and conformity," but retains a wide range of options available. The third scenario aims at that outcome.

3. Adequate Privacy in Public

It would greatly reduce the surveillance threat to self-realization if there were appropriate informational norms constraining governmental collection, distribution, and use of information. The necessary norms would implement an acceptable tradeoff between the need for privacy in public and the benefits of governmental surveillance in ways that facilitated the creation of privacy in public through coordination in informational-norm based interactions.

Such norms do not exist. We lack norms that allow governmental surveillance while constraining it in ways that ensure adequate privacy in public. One response is to substitute explicit legal regulation for norms. Norms, however, have at least three relevant advantages over laws. First, knowledge: parties to norms know what they are. You know the norm-implemented privacy tradeoffs without having to read a privacy policy, or master a statute or series of judicial decisions. Second, fine-grained, flexible constraints: norms constrain a wide variety of different types of information processing over a wide range of situations while allowing adjustments for different individual or contextual needs. It is difficult for explicit legal regulation to be similarly comprehensive, detailed, and flexible. Third, the recognition of privacy in public: informational norms facilitate the creation of privacy in public. No matter what the means, it is essential to constrain the governmental use of surveillance information in ways that enable the coordination necessary to create an adequate degree of privacy in public. Adequacy is a matter of allowing multifaceted selves to flourish; otherwise, we—our *selves*—become shadows of what we once were.

---

241. GREENWALD, *supra* note 4, at 195.

We conclude with Glen Greenwald's 2014 version of Schneier's 2007 question with which we began:

> [W]e stand at a historic crossroads. Will the digital age usher in the individual liberation and political freedoms that the Internet is uniquely capable of unleashing? Or will it bring about a system of omnipresent monitoring and control, beyond the dreams of even the greatest tyrants of the past? Right now, either path is possible. Our actions will determine where we end up.[242]

242. *Id.* at 6.