2015

Surveillance as Loss of Obscurity

Woodrow Hartzog
Boston University School of Law

Evan Selinger

Surveillance as Loss of Obscurity

Woodrow Hartzog*
Evan Selinger**

Table of Contents

I. Introduction

Everyone seems concerned about government surveillance, yet we have a hard time agreeing when and why it is a problem and what we should do about it. When is surveillance in public unjustified? Does metadata raise privacy concerns? Should encrypted devices have a backdoor for law enforcement officials? Despite increased attention, surveillance jurisprudence and theory still struggle for coherence.[1] Different kinds of surveillance are often not grouped together as part of the same problem, like facial recognition technologies and portals for viewing ISP records.

* Associate Professor, Samford University's Cumberland School of Law, Affiliate Scholar, The Center for Internet and Society at Stanford Law School.

** Professor of Philosophy, Rochester Institute of Technology. The authors wish to thank Julie Brill, Danielle Citron, Patrick Gamez, Melinda Gromely, Don Howard, Mark McKenna, and Neil Richards. The authors would also like to thank Lydia Wimberly and Megan Fitzpatrick for their research assistance.

1. *See infra* notes 14–15 and accompanying text (collecting cases).

Proposed remedies also vary according to who is the watcher, the thing being surveilled, and the regulatory system in place to monitor the surveillance. In short, a common thread for modern surveillance problems has been difficult to find.

At the heart of the surveillance debate are contested uses of technology that continuously and indiscriminately collect, use, and analyze information that people choose to share with others, such as automatic license plate readers that track all vehicles, software that scrapes and analyzes the social web, and drones that can effortlessly track multiple targets in public for long durations.[2] In these cases, questions arise as to whether privacy violations occur when technology makes formerly manpower-intensive legitimized surveillance cheap and easy—ostensibly too easy.

Yet, despite the widespread concern and extensive academic treatment of surveillance issues, the language and framing used in surveillance debate is diverse, inconsistent, and over-generalized.[3] When people try to identify what it means to live in a surveillance society, they usually say something like: "There is more data than ever before and it is increasingly easier for the government to access this data and understand what it means."

Theorists have responded in numerous ways, giving surveillance extensive academic attention. The literature links surveillance to issues of autonomy, trust, power, dignity, respect, identity, anonymity, disparate impact, and exploitation, among others.[4] Scholars have proposed theories based on property, intellectual privacy, quantitative privacy, and others to help understand why and how surveillance is dangerous.[5] Reform efforts have focused on pragmatism, bright-line time restrictions, curtilage, trespass, and a host of other strategies.[6]

In particular, concepts like the "plain view" and "third party" doctrines, which enable surveillance of things and activities

---

2. *See infra* notes 9–11 (listing modern surveillance technologies).

3. *See infra* notes 14–15 and accompanying text (collecting cases and discussing variance in judicial opinions regarding surveillance).

4. *See infra* notes 34–44 and accompanying text (summarizing academic discussion on surveillance).

5. *See infra* notes 138–141 (discussing the impact of surveillance on intellectual property).

6. *See infra* notes 34–44 and accompanying text (summarizing academic discussion on surveillance).

exposed or shared with others, conflict with modern notions of privacy. Most people bristle at the idea that there is absolutely "no privacy in public." Critics have assailed the notion of indiscriminate public surveillance. Yet, other than the still-developing "mosaic theory," which recognizes the revelatory power of aggregated surveillance, little headway has been made regarding reform for many modern forms of government surveillance.[7]

Ideas about preventing the surveillance society from going too far usually focus on three desirable outcomes: (1) prevent certain groups from ever having access to certain types of information; (2) prevent certain groups from being able to use certain types of information in select contexts or in certain ways; and (3) make it harder for certain groups to be able to access or interpret information.

Government surveillance debates primarily revolve around the third strategy—making government surveillance hard but possible. Government surveillance concerns are rarely about prohibiting the government from ever being able to access any particular information, save issues like professional confidences, evidentiary privileges, and rights to resist self-incrimination. Nor are government surveillance concerns primarily about preventing the government from discriminating against us on the basis of information it should not be allowed to use, unless there is debate about what data should be considered fair game for consideration when creating things like the no-fly list.

Instead, the main source of anxiety about government surveillance is about how easy it is for the government to access our information: how readily government agents can access our phones, our e-mail, our information stored in the cloud, our meta-data, our geo-location data, and the like. Big concerns also exist about how easily the government can combine readily accessible data to form revealing profiles.

We think the government's relative difficulty in finding information is central to advancing the debate over government surveillance. In this Article we argue that the concept of "obscurity," which deals with the transaction costs involved in

---

7. *See infra* notes 123–124 and accompanying text (explaining the mosaic theory).

finding or understanding information, is the key to understanding and uniting modern debates about government surveillance.[8] Obscurity can do several things for privacy theorists and policy-makers in the debate over government surveillance.

First, obscurity can explain why making surveillance hard but possible is the central issue in the government surveillance debates. Second, obscurity can be used to help identify different areas where transactions costs for surveillance are operative and explain why they are central components of the debate. Third, obscurity can explain why the solutions to the government surveillance problem revolve around a common dynamic: introducing more transaction costs through friction and inefficiency into process, whether it be legally through procedural requirements like warrants or technologies like robust encryption. Ultimately, obscurity can provide a clearer picture of why and when government surveillance is troubling. Appeals to obscurity can also cultivate an appreciation for why and how transaction costs might be introduced into domains that have until now been regulated by policies like the third-party doctrine.

Although these might seem like overly ambitious outcomes for applying a novel and fundamentally descriptive concept, the way we frame problems can affect how they are structured and resolved. Obscurity is a desirable locus for reform efforts because the concept translates well across different prescriptive surveillance theories. In part, this is because normative dimensions of surveillance theory have advanced more quickly than the vocabulary that is needed to identify when surveillance practices endanger values that the normative theories justify as being important to protect.

A benefit of obscurity discourse having widespread theoretical applicability is that it can further diverse reform goals. By agreeing on a common descriptive theory of surveillance, reform advocates have a common thread for reform efforts. Academics can use obscurity to support normative surveillance theories. For example, obscurity can enhance the quality of arguments for rights of "intellectual privacy" and "quantitative privacy."

---

8. *See infra* Part III (defining and discussing obscurity in the context of surveillance).

This Article proceeds in three parts. In Part II, we describe the failure of the law to form a consistent, holistic response to surveillance. We demonstrate that while justices, advocates, policy-makers, and citizens intuitively understand surveillance problems, they often struggle to articulate how or why such surveillance is problematic. This inability to clearly describe the problem and find coherence among the diverse theories of surveillance has hindered consensus for reform.

In Part III, we introduce the concept of obscurity and explain the important role that transaction costs for finding and understanding information have played in shaping our societal notions about privacy. We demonstrate that while the logic of obscurity preservation has been articulated in a number of judicial opinions regarding government surveillance, progress requires a more explicit adoption of the framing. In Part IV, we argue that obscurity should be the center of gravity for modern surveillance theory. As a descriptive concept, obscurity can explain when and how government surveillance is problematic. It provides a common thread for disparate surveillance theories. Finally, obscurity can be used to direct surveillance reform.

II. Surveillance and Theory: Many Concerns, Little Consensus, No Locus

Every week there is seemingly a new story concerning a troubling new surveillance practice or technology. Beyond the Snowden disclosures, the past few years have seen widespread use of cellphone-tower-mimicking technologies like the Stingray that allows police to intercept phone conversations,[9] expansion of the FBI's next generation facial-recognition technology system,[10]

9. *See* John Kelly, *Cellphone Data Spying: It's Not Just the NSA*, USA TODAY (June 13, 2014), http://www.usatoday.com/story/news/nation/2013/12/08/cellphone-data-spying-nsa-police/3902809 (last visited June 12, 2015) ("Armed with new technologies, including mobile devices that tap into cellphone data in real time, dozens of local and state police agencies are capturing information about thousands of cellphone users at a time, whether they are targets of an investigation or not . . . .") (on file with the Washington and Lee Law Review).

10. *See* Rishi Iyengar, *New FBI Software Can Process up to 52 Million Facial Images*, TIME (Sept. 17, 2014), http://time.com/3389559/fbi-facial-recognition-software-interstate-photo-system-ips-next-generation-identification-ngi (last visited June 12, 2015) ("A Freedom of Information Act lawsuit filed by the

license plate readers that allow both police and private parties to keep tabs on vehicles' whereabouts,[11] and drones are enabling more persistent and elusive public and private sector surveillance.[12] These stories raise a general anxiety over a surveillance nation, yet they are different enough not to be grouped together both in terms of why they are problematic, as well as what to do about them.

Facial-recognition technologies are often seen as problematic because it is impractical to hide your face when in public or change it as a surveillance countermeasure. Biometrics create a new class of "searchable" information. License plate readers, which simply record the location of a vehicle on a public road, create a different problem. Discussions surrounding license plate readers almost exclusively focus on the aggregated nature of such information. While observation of a single car's license plate is seen as freely permissible, effortlessly recording hundreds of thousands of such observations and discerning patterns over time create a separate problem.

---

foundation in April revealed that the system could process up to 52 million facial images, including millions of pictures taken for noncriminal purposes.") (on file with the Washington and Lee Law Review).

11. *See* Devlin Barrett, *U.S. Spies on Millions of Drivers*, WALL ST. J. (Jan. 26, 2015), http://www.wsj.com/articles/u-s-spies-on-millions-of-cars-1422314779 (last visited June 12, 2015) ("The Justice Department has been building a national database to track in real time the movement of vehicles around the U.S., a secret domestic intelligence-gathering program that scans and stores hundreds of millions of records about motorists, according to current and former officials and government documents.") (on file with the Washington and Lee Law Review).

12. *See* Tom Loftus, *Concerns Rise About Growing Use of Domestic Drones*, USA TODAY (July 18, 2013), http://www.usatoday.com/story/tech/2013/07/18/drone-concerns-rules-regulations/2552999 (last visited June 12, 2015) ("[G]overnment agencies and universities can apply to the FAA for a certificate of authority to fly a drone—large or small. Commercial drone usage is prohibited now but is expected to take off after September 2015, a deadline Congress gave the FAA to create a plan to integrate unmanned aircraft into the airspace.") (on file with the Washington and Lee Law Review); *see also* Dan Roberts, *FBI Admits to Using Surveillance Drones over US Soil*, THE GUARDIAN (June 19, 2013), http://www.theguardian.com/world/2013/jun/19/fbi-drones-domestic-surveillance (last visited June 12, 2015) ("However, the potential for growing drone use either in the US, or involving US citizens abroad, is an increasingly charged issue in Congress, and the FBI acknowledged there may need to be legal restrictions placed on their use to protect privacy.") (on file with the Washington and Lee Law Review).

Still different is drone surveillance, which is often categorized as a "peeping tom" problem.[13] Drones provide access to information that would have been unable or unlikely to be viewed by the naked eye before. Yet concerns about peeping drones are still different than debates surrounding cleavage, upskirt, and "creeper" photos in public. Here, the concern is not aggregation or newly enabled access to private spaces, but rather the fixation of a moment otherwise destined to be fleeting and forgotten. Unlike license plate readers, even one such instance can be problematic, even though people exposed themselves to the public. Yet, unlike peeping drones, cleavage and upskirt photos are often taken in public spaces.

Thus, modern surveillance can be problematic because it involves secrets, fleeting public exposure, aggregated information, and unchangeable biological identifiers. This is to say nothing of the traditionally problematic surveillance issues involving the interception or requisition of communications and stored information.

It is thus no surprise that it has been difficult to find a common center of gravity for surveillance policy and discourse. Focusing on aggregated information excludes consideration of single-instance surveillance. Focusing on the interception of communications can overshadow concerns about biometrics and genetic data. The lack of commonality among the many different issues has resulted in inconsistent and confusing policy, as well as discrete and diverse reform attempts.

For example, the law of public surveillance is increasingly a mess. Courts and policy-makers regularly affirm that there is no "privacy in public."[14] Entire concepts like the "public view" doctrine

---

13. *See* Mary-Ann Russon, *Are Flying Drones a Peeping Tom's Dream Tool?*, INT'L BUS. TIMES (June 11, 2014), http://www.ibtimes.co.uk/are-flying-drones-peeping-toms-dream-tool-1452278 (last visited June 12, 2015) ("Fears are growing that helicopter drones could be used to sexually harass women and take secret photographs of them.") (on file with the Washington and Lee Law Review).

14. *See, e.g.*, Chadwell v. Brewer, 59 F. Supp. 3d 756, 763 (W.D. Va. 2014) (discussing a public school teacher's expectation of privacy in an office he shared with another teacher); Order to Suppress Physical Evidence and Statements at 3, United States v. Cleveland, No. 18 DVM 1341 (Sup. Ct. D.C. Sept. 4, 2014), http://pdfserver.amlaw.com/nlj/Cleveland%20motion%20to%20sup press%20order.pdf ("This court finds that no individual clothed and positioned in such a manner in a public area in broad daylight in the presence of countless

and "third party" doctrine enable this truth in surveillance law.[15] The concept of a "reasonable expectation of privacy" is the critical and central concept that determines the scope of a number of different critical privacy protections.[16] It governs the scope of Fourth Amendment protections, as well as the torts of intrusion upon seclusion and the public disclosure of private facts, Fourth Amendment,[17] and the Electronic Communications Privacy Act (ECPA).[18] Courts and lawmakers have consistently established that there is no reasonable expectation of privacy in public information.[19]

In the landmark case *Katz v. United States*,[20] Justice Stewart wrote that "[w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection."[21] Yet the Justice then went on to muddy the

---

other individuals could have a reasonable expectation of privacy.").

15. *See* Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 563 (2009) ("[A] person cannot have a reasonable expectation of privacy in information disclosed to a third party."); *see also* Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311, 317 (2012) ("[C]onduct does not violate a reasonable expectation of privacy when it consists of observing the outside of property, observing what has already been exposed to the public, or observing public spaces where anyone may travel.").

16. *See supra* note 15 and accompanying text (discussing the role of a reasonable expectation of privacy in the fourth amendment context); *see also* Daniel J. Solove, *Fourth Amendment Pragmatism*, 51 B.C. L. REV. 1511, 1512 (2010) ("U.S. Supreme Court decisions applying the reasonable expectation of privacy test have been attacked as 'unstable' and 'illogical,' and even as engendering 'pandemonium.'").

17. *See e.g.*, Coolidge v. New Hampshire, 403 U.S. 443, 466 (1971) ("[T]he 'plain view' doctrine may not be used to extend a general exploratory search from one object to another until something incriminating at last emerges."); United States v. Miller, 425 U.S. 435, 443 (1976) ("[T]he Fourth Amendment does not prohibit the obtaining of information revealed to a third party . . . , even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.").

18. Electronic Communications Privacy Act, 18 U.S.C. § 2510 et seq. (2012).

19. *See* McCormick v. England, 494 S.E.2d 431, 437–38 (S.C. Ct. App. 1997) ("Invasion of privacy consists of the public disclosure of private facts about the plaintiff . . . . The defendant must intentionally reveal facts which are of no legitimate public interest, as there is *no right of privacy in public matters*." (emphasis added)); State v. Frost, 634 N.E.2d 272, 272 (Ohio Ct. App. 1994) ("The young ladies had no right of privacy at a public beach, and they probably expected to be observed in their bikini bathing suits.").

20. 389 U.S. 347 (1967).

21. *Id.* at 351 (citing Lewis v. United States, 385 U.S. 206, 210 (1966)).

conceptual waters by stating in the next sentence: "But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[22] *Katz* extended the pronounced trend of courts to bluntly exclaim that there can be no privacy in publicly shared information, yet completely failed to conceptualize public information. Commenting on the trend exacerbated by *Katz*, Brian Serr wrote:

> [T]he Court has made little effort to refine [the reasonable expectation of privacy] test; instead, the Court has focused primarily on the 'knowingly exposes to the public' language that the Katz majority used. Regrettably, the Court has severed that language from its context and used it as a talisman, ruling that any objects, statements, or activities exposed to the public—even if exposed only to a very limited degree—do not deserve fourth amendment protection.[23]

In *California v. Ciraolo*,[24] the Supreme Court wrote:

> The Fourth Amendment protection of the home has never been extended to require law enforcement officers to shield their eyes when passing by a home on public thoroughfares. Nor does the mere fact that an individual has taken measures to restrict some views of his activities preclude an officer's observations from a public vantage point where he has a right to be and which renders the activities clearly visible.[25]

The Court noted that because aircraft could reasonably be expected to fly over one's house at any time, "it is unreasonable for respondent to expect that his marijuana plants were constitutionally protected from being observed with the naked eye from an altitude of 1,000 feet."[26] The Court observed that "[t]he Fourth Amendment simply does not require the police traveling in the public airways at this altitude to obtain a warrant in order to observe what is visible to the naked eye."[27]

---

22. *Id.*

23. Brian J. Serr, *Great Expectations of Privacy: A New Model for Fourth Amendment Protection*, 73 MINN. L. REV. 583, 597–98 (1989).

24. 476 U.S. 207 (1986).

25. *Id.* at 213.

26. *Id.*

27. *Id.* at 215.

In *United States v. Knotts*,[28] the Supreme Court similarly held that "[a] person travelling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another."[29] The Court reasoned that walking down the street voluntarily conveys to "anyone who wanted to look the fact that he was travelling over particular roads in a particular direction, the fact of whatever stops he made, and the fact of his final destination when he exited from public roads onto private property."[30]

But this line of reasoning is problematic. Consider the confusion the "no privacy in public" assertion causes within the tort of public disclosure of private facts.[31] Courts often look to the location of where information is disclosed, yet there is no set definition for the term "public."[32] Public roads are obviously public, but what about indoor shopping malls? Offices in buildings? When are structures with four walls and a roof "public?"

Academic and societal criticism has also failed to converge around a common discourse or set of principles for critique and reform. While such different theories and approaches are useful, the lack of common ground means that possibly related topics are spoken of in different ways and treated differently in law and policy.

For example, scholars and the general public have revolted at the idea that there is no privacy in public and that the law should support such a notion.[33] But the logic of such criticism and proposed reform is diverse. For example, Andrew Guthrie

---

28. 460 U.S. 276 (1983).

29. *Id.* at 281–82.

30. *Id.*

31. *See* Diane L. Zimmerman, *Requiem for a Heavyweight: A Farewell to Warren and Brandeis's Privacy Tort*, 68 CORNELL L. REV. 291, 347 (1983) (citing numerous court decisions stating "that information individuals reveal about themselves in public places is by definition not private").

32. *See id.* (demonstrating the difficulty of distinguishing public places from private places).

33. *See* Andrew E. Taslitz, *The Fourth Amendment in the Twenty-First Century: Technology, Privacy, and Human Emotions*, 65 L. & CONTEMP. PROBS. 125, 169 (2002) ("Privacy, when defined as the boundary-maintenance necessary to individual and group definition, recognizes . . . that the 'private' can happen in 'public.' We do not shed all privacy expectations simply because we walk on a public street, or enter a classroom, or attend a ball game.").

Ferguson has proposed looking to the curtilage concept to resolve problematic questions of public surveillance.[34] According to Ferguson, "the theory of personal curtilage turns on persons being able to control the constitutionally protected areas of their lives in public by signifying that they intend for an area to be secure from physical and sense-enhancing invasion."[35] This account of surveillance focuses on concepts like property and control.[36]

For Helen Nissenbaum, public surveillance is all about context. Nissenbaum has theorized that privacy violations occur when "context-relative informational norms" are not respected when sharing information.[37] In proposing a theory of privacy as contextual integrity, Nissenbaum has proposed that "when violations of norms are widespread and systematic as in public surveillance, when strong incentives of self-interest are behind these violations, when the parties involved are of radically unequal power and wealth, then the violations take on political significance and call for political response."[38]

In addressing the notion of privacy in public, Joel Reidenbuerg has proposed:

> [T]he transformation of information flows through three stages of development, which fundamentally undermines the concept of a 'reasonable expectation of privacy.' Information that was once private through obscurity now becomes technologically accessible. Information that was once merely accessible now becomes transparent and receives wide publicity. These

34. *See, e.g.*, Andrew Guthrie Ferguson, *Personal Curtilage: Fourth Amendment Security in Public*, 55 WM. & MARY L. REV. 1283, 1290 (2014) ("This Article applies the theory of Fourth Amendment curtilage to persons acting in public."). According to Ferguson, "[c]urtilage has long been understood as a legal fiction that expands the protection of the home beyond the formal structures of the house. Curtilage recognizes a buffer zone beyond the four walls of the home that deserves protection even in areas observable to the public." *Id.*

35. *Id.* at 1287–88.

36. *See id.* ("Based on custom and law protecting against both nosy neighbors and the government, courts defined curtilage by the actions the property owner took to signal a protected space.").

37. HELEN NISSENBAUM, PRIVACY IN CONTEXT 129 (2010) (stating that the framework of contextual integrity provides that "finely calibrated systems of social norms, or rules, govern the flow of personal information in distinct social contexts (e.g., education, health care, and politics)").

38. Helen Nissenbaum, *Privacy as Contextual Integrity*, 79 WASH. L. REV. 119, 156 (2004).

> parameter changes no longer fit within traditional court jurisprudence on privacy."[39]

According to Reidenberg, "constitutional democracy depends on spheres of privacy in public to preserve public safety and fair governance."[40] To create those spheres of privacy in public, Reidenberg proposed that "privacy protection be framed in terms of 'governance-related' and 'nongovernance-related' acts."[41] Thus, Reidenberg's account of surveillance is dependent upon the nature of the acts being surveilled.

Chris Slobogin has framed the issue of privacy in public as one of anonymity.[42] In a different article, Slobogin proposes a solution to the problem of aggregated pieces of surveillance based upon the proportionality principle, "the idea that the justification for a search should be roughly proportional to the intrusiveness of the search" and "John Hart Ely's political process theory."[43] According to Slobogin, "as applied to searches, this theory counsels that courts should generally defer to legislation authorizing searches of groups when the affected groups have meaningful access to the legislative process and the search is implemented in an even-handed fashion."[44]

---

39. Joel R. Reidenburg, *Privacy in Public*, 69 U. MIAMI L. REV. 141, 143 (2014).

40. *Id.*

41. *Id.*

42. *See* Christopher Slobogin, *Public Privacy: Camera Surveillance of Public Places and the Right to Anonymity*, 72 MISS. L.J. 213, 217 (2002) ("The Fourth Amendment should be construed to recognize the right to public anonymity as a part of the privacy expectations that, to use the Supreme Court's well-known phrase, 'society is prepared to recognize as reasonable.'").

43. Christopher Slobogin, *Making the Most of* United States v. Jones *in a Surveillance Society: A Statutory Implementation of Mosaic Theory*, 8 DUKE J. CONST. L. & PUB. POL'Y 1, 4 (2012).

44. *Id.* Slobogin proposes specific language for the codification as follows:

> (a) A targeted public search that lasts longer than 48 hours in aggregate requires probable cause, and a warrant unless exigent circumstances exist.
>
> (b) A targeted public search that lasts longer than 20 minutes in aggregate but no longer than 48 hours in aggregate requires reasonable suspicion, and a court order unless exigent circumstances exist.
>
> (c) A targeted public search that does not last longer than 20 minutes in aggregate may occur at a law enforcement officer's discretion whenever the officer believes in good faith that the search can

Jeffrey Skopek also couches the surveillance debate and proposed resolutions in terms of anonymity. Skopek argued that the failure of the law to protect privacy in public is the result of confusion between anonymity and privacy.[45] These scholars are just a few of the many voices in surveillance law, policy, and theory with diverse views on when and why surveillance is a problem and what we should do about it.

But this diversity makes it hard for courts and lawmakers to create coherent surveillance jurisprudence. Often, they must adhere to one account or another. A common ground for the modern surveillance debate would be useful. But first we must talk about "privacy" in a different way. Instead of focusing on traditional notions of "private" and "public," we propose that the concept of obscurity, which deals with the difficulty and probability of discovering or understanding information, is more effective than traditional frames for the surveillance debate. Obscurity sits along a continuum. Appeals to the concept can mitigate the atomistic nature of modern surveillance policy and discourse and can help resolve our tendency to fall back into the public privacy divide.

III. An Obscurity Primer

In this Part, we develop our theory of surveillance as loss of obscurity. According to the *Oxford English Dictionary*, the word "obscurity" has been in circulation for quite some time.[46] Its original meaning, the "quality or condition of not being clearly known or understood," dates back to 1474, and by 1495 it also

---

accomplish a legitimate law enforcement objective.

Id. at 24.

45. See Jeffrey M. Skopek, *Reasonable Expectations of Anonymity*, 101 VA. L. REV. (forthcoming 2015), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2523393&download=yes ("The problem with the public exposure and third party doctrines is not only that they fail to recognize that a piece of personal information can be protected in varying degrees . . . . In addition, and more fundamentally, they conflate two distinct forms that this protection can take: privacy and anonymity.").

46. *See* OXFORD ENG. DICTIONARY (3d ed. 2004) (defining "obscurity"), *available at* www.oed.com/view/Entry/129848?redirectedFrom=obscurity#eid34119781.

meant "a wholly or partially unintelligible expression."[47] In the early part of the 16th century, when Gavin Douglas famously translated Virgil's *The Aeneid*, obscurity became associated with "uncertainty of meaning."[48] And while members of our contemporary fame-obsessed society use obscurity to refer to "the quality or condition of being unknown" and an "unknown person" or "unknown thing," their etymologies respectively begin in 1578 and 1822.[49]

The law, however, has its own specialized lexicon for obscurity. The canonical starting point for explicit debate about "practical obscurity" in the American judicial system is the 1989 ruling of *U.S. Department of Justice v. Reporters Committee for Freedom of the Press*.[50] There the Supreme Court recognized a privacy interest in information that is publicly available, but nevertheless difficult to obtain.[51]

Specifically, the Court determined that the Freedom of Information Act requirements do not compel the federal government to use its criminal records database to expedite access to rap sheets so that inquirers are spared effort and expense; justice is not violated if they have to seek out the information from inconveniently located places, such as courthouses' files.[52] In delivering the Court's opinion, Justice John Paul Stevens writes:

> In sum, the fact that 'an event is not wholly 'private' does not mean that an individual has no interests in limiting disclosure or dissemination of the information' . . . the substantial character of that interest is affected by the fact that in today's

47. *Id.*

48. *Id.*

49. *Id.*

50. 489 U.S. 749 (1989). In the domain of cybersecurity, obscurity has a technical meaning as well. There it involves "hiding information": concealing vulnerabilities, so that others cannot take advantage of those weaknesses, and "deliberately suppressing general information about a system to make things more difficult for adversaries, hackers, and third parties to discover flaws in a system." EDWARD AMOROSO, CYBER ATTACKS: PROTECTING NATIONAL INFRASTRUCTURE 171 (2012).

51. *See United States v. Reporters Comm.*, 489 U.S. 749, 750 (1989) (recognizing a strong privacy interest in maintaining the "practical obscurity" of a rap sheet).

52. *See id.* ("[T]he privacy interest in maintaining the rap sheet's 'practical obscurity' is always at its apex while the FOIA-based public interest in disclosure is at its nadir.").

> society the computer can accumulate and store information that would otherwise have surely been forgotten long before a person attains age 80, when the FBI's rap sheets are discarded.[53]

Unfortunately, *Reporters Committee* turned out to be, thus far, the legal apex for obscurity argumentation.[54] In subsequent years, there has been only intermittent case law acknowledgement that the logic underlying the decision is valid and has broader applicability.[55]

For example, although the term "obscurity" is not used in the Supreme Court of New York case *Bursac v. Suozzi,*[56] the ruling does cite privacy interests acknowledged in *Reporters Committee*.[57] In this instance, the court determined that while DWI arrests are a matter of public record, Nassau County Executive Thomas Suozzi went too far in creating an online "Wall of Shame," containing mugshots and names of people who were arrested in his country for the offense.[58]

According to Judge William R. LaMarca:

> It is the scope and permanency of public disclosure on the Internet by a governmental agency that distinguishes the County's "Wall of Shame" from traditional and regular forms of reporting and publication such as print media. The County Executive's campaign of publicizing DWI arrests serves a legitimate purpose but the use of specific identifying information on the Internet, with its endless implications, is of concern to the court.[59]

Simply put, because publishing DWI arrests online can lead to "limitless and eternal notoriety, without any controls," the court

---

53. *Id.* at 770.

54. *See, e.g.*, Woodrow Hartzog & Frederic D. Stutzman, *The Case for Online Obscurity*, 101 CAL. L. REV. 1, 21–24 (2012) (discussing the reluctance of courts to expand upon the "practical obscurity" concept articulated in *Reporters Committee*).

55. *See id.* at 21–22 ("Beyond a general sense that shared or available information does not always constitute public information, courts have had a difficult time expanding on the concept.").

56. 868 N.Y.S.2d 470 (N.Y. Sup. Ct. 2008).

57. *See id.* at 479 ("The Internet has no sunset and postings on it will last and be available until some person purges the Web site, perhaps in decades to come.").

58. *Id.* at 473–74.

59. *Id*. at 480.

concluded that the risk is too great that unfair harms will come to those listed on the digital wall.[60] Beyond undermining the constitutionally protected due process that should be afforded to those profiled (by presenting potential members of a jury with incriminating portraits), the information too easily induces bias and can tempt potential employers and landlords to abuse their power in perpetuity.[61]

With cases like these in mind, we have proposed our own definition of obscurity that is privacy-oriented: "Obscurity is the idea that when information is hard to obtain or understand, it is, to some degree, safe."[62] Obscurity considerations can play a role in protecting all forms of communication, and "online obscurity" exists when at least one of the four "key factors" is missing that play a crucial role in discovering or comprehending information: "(1) search visibility, (2) unprotected access, (3) identification, and (4) clarity."[63] Because there are many ways to manipulate these factors, different strategies can make online disclosures more obscure. For example:

> [S]haring ideas on platforms that are invisible to search engines; using privacy settings and other access controls; withholding your real name and speaking anonymously or identifying yourself with a pseudonym; disclosing information in coded ways that only a limited audience will grasp; or transmitting content that is encrypted or temporarily accessible through an ephemeral conduit, like Snapchat, the photo

60. *Id.* at 481.

61. *See id.* at 480 ("It is the scope and permanence of public disclosure on the Internet by a government agency that distinguishes the County's 'Wall of Shame' from traditional and regular forms of reporting and publication such as print media.").

62. Woodrow Hartzog & Evan Selinger, *Obscurity: A Better Way to Think About Your Data Than "Privacy,"* THE ATLANTIC (Jan. 17 2013), http://www.theatlantic.com/technology/archive/2013/01/obscurity-a-better-way-to-think-about-your-data-than-privacy/267283/ (last visited June 12, 2015) (on file with the Washington and Lee Law Review); s*ee also* Evan Selinger & Woodrow Hartzog, *Obscurity and Privacy*, *in* ROUTELEDGE COMPANION TO PHILOSOPHY OF TECHNOLOGY (Joseph Pitt & Ashley Shew eds., 2014), ("Obscurity is the idea that information is safe—at least to some degree—when it is hard to obtain or understand.").

63. Hartzog & Stutzman, *supra* note 54, at 2.

> messaging application that can delete information within seconds after the recipient views it.[64]

While anyone can use these strategies and related ones, discrete individual action is not the only scale for adding obscurity to the online information ecology. Consider the recent policy debate over Europe's so-called "right to be forgotten" and America's so-called "erasure" laws.[65] We believe that some of the discussions have gotten derailed when partisans insist that the ability to delete links to information stored on Google or to remove information minors previously posted on websites is tantamount to historical revisionism—a prohibition that prevents others from noticing that someone once wrote something or had something written about him or her.

To correct these exaggerated interpretations, we have argued the endeavors should be fundamentally construed as obscurity-promoting initiatives that make it hard (or harder), but not impossible, to discover irrelevant, inadequate, and embarrassing details.[66] After all, in the former case, original source material is

---

64. Selinger & Hartzog, *supra* note 62.

65. *See, e.g.*, Woodrow Hartzog, *A Stronger Online Eraser Law Would Be a Mistake*, NEW SCIENTIST (Nov. 12, 2013), http://www.newscientist.com/article/mg22029420.200-a-stronger-online-eraser-law-would-be-a-mistake.html#.VQyHa47F_E8 (last visited June 12, 2015) ("So I firmly believe the goal of erasing unremarkable self-disclosures is more palatable than the broad 'right to be forgotten' proposals by the EU and France. California's effort is closer to a 'right to hide.'") (on file with the Washington and Lee Law Review); Eric Posner, *We All Have a Right To Be Forgotten*, SLATE (May 14, 2014), http://www.slate.com/articles/news_and_politics/view_from_chicago/2014/05/the_european_right_to_be_forgotten_is_just_what_the_internet_needs.html (last visited June 12, 2015) ("It's not a right to be purged from the memory of people who know you, but rather to control how information about you appears online.") (on file with the Washington and Lee Law Review); Jonathan Zittrain, *Don't Force Google to "Forget"*, N.Y. TIMES (May 14, 2014), http://www.nytimes.com/2014/05/15/opinion/dont-force-google-to-forget.html?_r=2 (last visited June 12, 2015) (arguing the Europe's "right to be forgotten" is both too broad in that it "allows individuals to impede access to facts about themselves found in public documents" and too narrow in that it "doesn't require that unwanted information be removed from the web") (on file with the Washington and Lee Law Review).

66. *See* Hartzog & Selinger, *supra* note 62 ("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."); Selinger & Hartzog, *supra* note 62 ("When information is hard to come by, the only people who will seize upon it are those with sufficient motivation to expend the necessary effort and resources.").

left intact, while the latter instance does not obliterate third party re-posts.[67] Although appeals to authority have questionable evidentiary weight, it is still worth noting that Federal Trade Commissioner Julie Brill has used similar framing.[68]

At its core, our account of obscurity is predicated upon a causal view of human behavior: people are routinely deterred from pursuing goals that require expending effort or assets when they lack the requisite motivation or resources. The main causal claim at the heart of obscurity theory, therefore, is that when information is difficult to acquire or burdensome to interpret, the only people who will be inclined to do the detective work are those who deem the expense an acceptable cost.

Because many factors can go into determining when a person judges the expense of obscurity-minimizing measures as reasonable to incur, calculations about who will be thwarted by obscurity-enhancing techniques are always probabilistic in nature. Creating restraints by adding transaction costs can never provide the peace of mind offered by absolute safeguards that guarantee competent and determined parties—including busybodies, enemies, aggrieved members of a community, hackers, and government agencies—are definitively unable to obtain or decipher disclosures we wish to selectively share. But then again, it is doubtful that such foolproof safeguards actually exist. As Paul Ohm rightly notes, "No technology is perfect, and advocates who

---

67. *See* Evan Selinger & Woodrow Hartzog, *Google Can't Forget You, But It Should Make You Hard to Find*, WIRED (May 20, 2014), http://www.wired.com/2014/05/google-cant-forget-you-but-it-should-make-you-hard-to-find/ (last visited June 13, 2015) ("This debate is not and should not be about forgetting or disappearing in the traditional sense. Instead, let's recognize that the talk about forgetting and disappearing is really concern about the concept of obscurity in the protection of our personal information.") (on file with the Washington and Lee Law Review).

68. *See* JULIE BRILL, PRIVACY IN THE AGE OF OMNISCIENCE: APPROACHES IN THE UNITED STATES AND EUROPE 2 (2014) ("Here, we can all agree that as the Age of Omniscience descends upon us, we can and will find ways to protect individual privacy."); *see also* Evan Selinger & Woodrow Hartzog, *Why You Have the Right to Obscurity*, CHRISTIAN SCI. MONITOR (Apr. 15, 2015), http://www.csmonitor.com/World/Passcode/Passcode-Voices/2015/0415/Why-you-have-the-right-to-obscurity (last visited Sept. 6, 2015) (interviewing Commissioner Brill) (on file with the Washington and Lee Law Review).

comment on privacy and technology in truth almost never advocate for perfect privacy . . . ."[69]

Research across the disciplines, both old and new, supports our causal intuitions. Modern scholarship critiques the recent obsession over "frictionless sharing" via social media.[70] But as far back as antiquity, people testified that expediency is a seductive temptation. Take Plato's famous discussion of the story Gyges in *The Republic* (360 B.C.E.), a parable that is presented so we can consider why a mythical shepherd behaved badly by using a ring of invisibility to effortlessly kill a king and seduce his wife, the queen.[71] Plato was not simply articulating why moral deliberation is required to reject egoism and the realist doctrine that justice is the advantage of the stronger. He also was identifying frictionless experience as a corruptive force.[72]

Contemporary discussion about the ethics of using consumer technology often revolves around concern about diminished effort diminishing our experiences. For example, Albert Borgmann, a preeminent philosopher of technology, argues that the prevalence of cheap consumer devices designed to disburden us from hard work by providing safe, easy, and instantaneous opportunities for satisfaction significantly impedes our desire to develop the type of robust character needed to pursue a truly meaningful life: the availability of fast food and microwave dinners disinclines families from preparing meals from scratch; and the ease of being entertained by televisual media incentivizes us to avoid more taxing activities, like reading.[73] In the same spirit, one of us has

---

69. Paul Ohm, *Good Enough Privacy*, 2008 U. CHI. LEGAL F. 1 (2008).

70. *See, e.g.*, Neil Richards, *The Perils of Social Reading*, 101 GEO. L.J. 689, 713 (2013) ("There are just three problems with making frictionless sharing of reader records our default: Frictionless sharing isn't frictionless, it isn't really sharing, and it's corrosive of intellectual privacy and intellectual freedom."); William McGeveran, *The Law of Friction*, 2013 U. CHI. LEGAL F. 15, 15–17 (2013) ("[T]he word 'friction' has another meaning: it describes the forces that impede individuals from disclosing personal information when they use online services. . . . [M]any implementations of frictionless architecture have gone too far, potentially invading privacy and drowning useful information in a tide of meaningless spam.").

71. *See* JOHN KAAG & SARAH KREPS, DRONE WARFARE 110 (2014) (recounting the story of Gyges).

72. *See id.* at 109–10 ("Even when it is incredibly easy, expediency is not necessarily a virtue.").

73. *See generally* ALBERT BORGMANN, TECHNOLOGY AND CHARACTER OF

argued that technological norms that demonize inefficient communication undermine the care and respect that etiquette is meant to inspire, and automated forms of communication that appreciably lessen thought and intentionality can diminish both autonomy and conscientiousness.[74]

The ethical stakes of altering effort are not limited to the effects of using commodities. They also extend to a vast range of policy issues. For example, in their account of "nudging," behavioral economist Richard Thaler and legal scholar Cass Sunstein argue that because humans are prone to being influenced by the cognitive bias of inertia, it is incumbent upon designers to help us avoid doing self-sabotaging things by creating sticky defaults that capitalize on our laziness.[75]

For example, providing small plates in cafeterias will make it easier for people to avoid overeating because many will not bother to wait in line for seconds. Retirement plans that automatically enroll employees will minimize the regret that people come to experience after realizing that being deterred by having to fill out an opt-in form and submitting it to human resources and resulting in them being financially unprepared to retire. Requiring driver's license applicants to decide whether or not to be organ donors will

---

CONTEMPORARY LIFE: A PHILOSOPHICAL INQUIRY (1984) (arguing that overreliance on technology leads to a life dominated by effortless and thoughtless consumption).

74. *See* Evan Selinger, *We're Turning Digital Natives into Etiquette Sociopaths*, WIRED (Mar. 26, 2014), http://www.wired.com/2013/03/digital-natives-etiquette-be-damned/ (last visited June 13, 2015) ("[W]hile living according to the gospel of technological efficiency and frictionless sharing is fine as a Silicon Valley innovation ethos, it makes for a downright depressing social ethic.") (on file with the Washington and Lee Law Review); Evan Selinger, *Will Autocomplete Make You Too Predictable?*, BBC FUTURE (Jan. 15, 2015), http://www.bbc.com/future/story/20150115-is-autocorrect-making-you-boring (last visited June 13, 2015) ("[B]y encouraging us not to think too deeply about our words, predictive technology may subtly change how we interact with one another. As communication becomes less of an intentional act, we give others more algorithm and less of ourselves.") (on file with the Washington and Lee Law Review).

75. *See generally* RICHARD H. THALER & CASS R. SUNSTEIN, NUDGE: IMPROVING DECISIONS ABOUT HEALTH, WEALTH, AND HAPPINESS (2008) (offering advice on preventing common mistakes based on research from fields of behavioral science and economics).

help them more readily actualize their altruistic intentions than if they faced opt-in schemes.[76]

And in their attempt to move debates about warfare beyond the concerns typically expressed over international law and local political processes, philosopher John Kaag and political scientist Sarah Kreps insist that drone strikes can minimize so many expenses for the United States—not just economic costs, but also in terms of potentially saving many soldiers' lives—that the country is at risk of embracing a moral hazard whereby the problem of "dirty hands" gets magnified, while citizens are shielded from its reality and consequences.[77]

One of the most important things to keep in mind when seeing situations as calling for obscurity-enhancing strategies is that obscurity is not an all-or-nothing state of affairs. Rather, obscure statements exist on a nuanced continuum of disclosure wherein we enter into public and semi-public settings, but aim to limit our communication to select audiences. Because these are instances where we volunteer thoughts, beliefs, and feelings, pursuing obscurity clearly cannot be the same thing as aiming for total secrecy.

And yet, at the same time, when obscurity considerations are in play we are not inviting everyone in the world to know our business, nor are we demonstrating allegiance to the ideal of a totally transparent life. Hence, one of us has argued that "[o]bscurity explains why we are comfortable talking about personal information in a crowded restaurant and posting personal information to a restricted number of people within online communities."[78] Indeed, "[a] significant portion of our everyday interaction places us into a zone of obscurity, where our identity

---

76. One of us has contested Thaler and Sunstein's approach to organ donation. *See generally* Kyle Powys Whyte, Evan Selinger, Arthur L. Caplan & Jathan Sadowski, *Nudge, Nudge or Shove, Shove—the Right Way for Nudges to Increase the Supply of Donated Cadaver Organs*, 12:2 AM. J. BIOETHICS 32 (2012) (arguing that Thaler and Sunstein's approach fails to appreciate how perceptions of meaning can influence people's responses to nudges).

77. *See* KAAG & KREPS, *supra* note 72, at 109–10 ("[B]ut the story also suggests that it is difficult to blame a person whom you can't see, and even harder to bring them to justice. In these disturbing cases, a wicked act can go unexamined and therefore unpunished.").

78. Woodrow Hartzog, *The Fight to Frame Privacy*, 111 MICH. L. REV. 1021, 1038 (2013).

and personal context are unknown to those we interact with or share common space."[79] Socialization typically depends on some ability to manage the accessibility and comprehension of social exchanges by outsiders, the loss of which can be quite harmful.[80]

Obscurity is not a contemporary phenomenon. Indeed, social norms have historically developed around it. Jim Harper correctly notes:

> Practical obscurity has long ensured that even nonprivate information is not widely shared. An endless array of social, legal, and economic practices has developed around the assumption that the information collected about people will remain practically obscure. The things we wear, the places we go, the people we see, the things we say, and the things we buy have all been chosen in the best under the umbrella of practical obscurity.[81]

While Harper makes descriptive observations about what has been the case, Harry Surden has gone a step further and argued that the practical limitations that make obscurity possible—including the "latent structural constraints" of transaction costs—have historically created a psychological sense that citizens are protected by "structural rights."[82]

---

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

80. *See generally* IRWIN ALTMAN, THE ENVIRONMENT AND SOCIAL BEHAVIOR (1975) (analyzing the concepts of privacy, crowding, territory, and personal space, with regard to human behavior); ERVING GOFFMAN, THE PRESENTATION OF SELF IN EVERYDAY LIFE (1959) (studying human behavior in social situations and the way we appear to others); ERVING GOFFMAN, BEHAVIOR IN PUBLIC PLACES: NOTES ON THE SOCIAL ORGANIZATION OF GATHERINGS (1966) (discussing social psychology research in social settings); SANDRA PETRONIO, BOUNDARIES OF PRIVACY: DIALECTICS OF DISCOURSE (2002) (offering a practical theory for why people make decisions about revealing and concealing private information); Erving Goffman, *Felicity's Condition*, 89 AM. J. SOC. 1, 51 (1983) (reviewing work in sociolinguistics, pragmatics, and conversational analysis in the sociological study of social interaction); Geoffrey A. Fowler, *When the Most Personal Secrets Get Outed on Facebook*, WALL ST. J. (Oct. 13, 2012), http://online.wsj.com/article/SB10000872396390444165804578008740578200224.html (last visited June 12, 2015) (describing the harmful effects of inadvertently disclosing information known only to a small group on the social network site Facebook) (on file with the Washington and Lee Law Review).

81. JIM HARPER, IDENTITY CRISIS: HOW IDENTIFICATION IS OVERUSED AND MISUNDERSTOOD 162 (2006).

82. *See* Harry Surden, *Structural Rights in Privacy*, 60 SMU L. REV. 1605, 1607 (2007) ("In the privacy context, society implicitly relies upon non-legal

This special class of rights is a matter of legally codified, positive entitlements. Instead, structural rights are pervasive social expectations about how information can be accessed, interpreted, and shared. The crucial thing, Surden insists, is that when structural rights are sufficiently strong and reliably present, they can contribute to a climate where it seems unnecessary for society to take further legal steps to protect our interests.[83] Consequently, lawmakers need to avoid succumbing to the reductionist temptation of believing that all of the protections citizens expect to be in place have been formally assigned legal rights.

Given the nuance and historical depth of obscurity, appeals to the concept can shed new light on a range of privacy debates that have been theoretically limited by seemingly intractable binary terms. In normative discourse, as well as privacy law and policy, there is a tendency to consider information as either public or private.[84] "This maligned on/off approach to privacy has been called the 'public-private dichotomy' or 'secrecy paradigm.'"[85]

Daniel Solove describes the secrecy paradigm as an understanding of privacy based on concealment preventing others from invading one's hidden world.[86] Under this conception, disclosed information is no longer concealed and thus, no longer private. Sharon Sandeen notes that this "vision of privacy makes it difficult for individuals to protect personal information once it has been shared with others."[87] Solove argued that the secrecy

---

regulators to prevent a large number of unwanted behaviors.").

83. *See id.* at 1609 ("To the extent that society depends upon the presence of these costs to reliably inhibit a potential privacy-violating activity, their dissipation results in a sudden regulatory shift, leaving these interests unprotected.").

84. *See* Hartzog & Stutzman, *supra* note 54, at 17 ("[M]any conflicts seem to stem from one problem—individuals have complex notions of privacy in regard to personal information but the law tends to treat that information only two ways: public or private.").

85. *Id.*

86. *See* DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 42 (2004) ("Privacy is about concealment, and it is invaded by watching and by public disclosure of confidential information.").

87. Sharon K. Sandeen, *Relative Privacy: What Privacy Advocates Can Learn from Trade Secret Law*, 6 MICH. ST. L. REV. 667, 694 (2006).

paradigm "fails to recognize that individuals want to keep things private from some people but not others."[88]

Disclosing information to some, but not all, is a difficult task. Solove asserts that not all private activities are pure secrets

> in the sense that they occur in isolation and in hidden corners. When we talk in a restaurant, we do not expect to be listened to. A person may buy condoms or hemorrhoid medication in a store open to the public, but certainly expects these purchases to be private activities.[89]

Solove holds that, contrary to the notion that information in public records cannot be private, "there is a considerable loss of privacy by plucking inaccessible facts buried in some obscure [public] document and broadcasting them to the world on the evening news. Privacy can be infringed even if no secrets are revealed and even if nobody is watching us."[90]

It is worth asking whether complete secrecy is even possible in a networked world. Solove posits that life in the information age "often involves exchanging information with third parties, such as phone companies, Internet service providers, cable companies, merchants, and so on. Thus, clinging to the notion of privacy as total secrecy would mean the practical extinction of privacy in today's world."[91]

Other scholars have advocated similar obscurity-related pursuits. For example, Rebecca Green expressed concern that digital-age citizens who sign petitions and contribute to political causes by donating small amounts of money are at heightened risk of having undesired parties monitor their views.[92] While those of us who are comfortable proclaiming our political beliefs to anyone who will listen will not be deterred by this possibility, others who prefer to be discrete may become less willing to participate in basic

---

88. SOLOVE, *supra* note 86, at 44.

89. *Id.*

90. *Id.*

91. Daniel Solove, *Conceptualizing Privacy*, 90 CAL. L. REV. 1087, 1152 (2002).

92. *See* Rebecca Green, *Petitions, Privacy, and Political Obscurity*, 85 TEMP. L. REV. 367, 367 (2013) ("But if political privacy does matter, if the reaction to amplified exposure in petition signing does dissuade people from signing petitions, a basic part of our political process will be threatened.").

political processes—especially when troubling outcomes can arise if the wrong crowd gets wind of where our sympathies lie.[93]

As Green points out, groups who are opposed to certain ideas or outcomes can target supporters for harassment.[94] Among other things, politically motivated groups can circulate lists that reveal who signed petitions alongside other publically available information, such as the signatories' addresses, phone numbers, and even links to online maps that give directions to their homes.[95]

Ultimately, Green contends that if we reach undesirable levels of concern, society will need to acknowledge that a threat to "political privacy" has arisen from lost "political obscurity." On a descriptive level, she defines the term as follows:

> Political obscurity refers to the state of one's political preferences being shrouded or otherwise difficult to discern or distinguish by others. A person enjoys political obscurity when she can go about her day as she so chooses without others perceiving or otherwise determining the nature of her political views. The politically obscure person is able to control and manage the extent of disassociation from the political views she holds (or once held) or political actions taken in the present and in the past.[96]

Prescriptively, then, if political obscurity were viewed as a right, it would be understood as "the fundamental right to exist without one's political preferences being continuously recorded."[97]

At the other end of the spectrum, there is skepticism about the possibility of preventing the death of obscurity, as well as concern that proposals for protecting obscurity are misguided. Some insist that technological development makes appeals to obscurity antiquated. Anita Allen writes:

> The *Reporter's Committee* case . . . is also significant today as a kind of swan song, maybe a dirge. Thanks to electronic records,

---

93. *See id.* at 386 ("Growing empirical evidence suggests that waning political obscurity threatens petitioning.").

94. *See, e.g.*, *id.* ("The plaintiffs feared this targeted Internet dissemination would effectively become a blueprint for harassment and discrimination." (internal quotation marks omitted)).

95. *See id.* at 400 (describing the ability of political organizers to purchase targeted lists of likely petition signers).

96. *Id.* at 373.

97. *Id.*

> the Internet and search engines, the vaunted "practical obscurity" of data is soon to be a memory. Data once resigned to the dustbin of history is now at anyone's fingertips . . . . Bad behavior today, or unwise or inadvertent disclosures, are not forgotten; they will never become practically obscure.[98]

Others acknowledge that the concept of "obscurity" adds nuance to the privacy lexicon but doubt its legal relevance. Brian Wassom claims, "It is difficult to envision how obscurity could be lawfully enforced in a legal framework that forbids government restrictions on speech."[99]

Others still explicitly reject appeals to obscurity to justify the law-restricting endeavors for collecting and reporting truthful disclosures "to prevent a perceived, potential harm to someone's privacy interests."[100] In this context, it has been asserted that obscurity claims depart too strongly from established precedent, including the third-party doctrine, the logic underlying the Supreme Court's interpretation of the privacy of the home in its discussions of the Fourth Amendment's exclusionary rule, and the Supreme Court's rejection of privacy interests existing for things done in "plain view" or "open fields."[101] It has also been argued that obscurity claims suffer from the twin maladies of overstating harms and understating the value of transparency.[102]

There also are issue-specific rejections of proposals that are grounded in obscurity ideals. For example, it has been argued that

---

98. ANITA ALLEN, UNPOPULAR PRIVACY: WHAT MUST WE HIDE? 162 (2011).

99. BRIAN WASSOM, AUGMENTED REALITY LAW, PRIVACY, AND ETHICS: LAW, SOCIETY, AND EMERGING AR TECHNOLOGIES 46 (2014).

100. Heidi Reamer Anderson, *The Mythical Right to Obscurity: A Pragmatic Defense of No Privacy in Public*, 7 I/S: J.L. & POL'Y FOR INFO. SOC'Y 543, 549 (2011); *see also* Robert G. Larson III, *Forgetting the First Amendment: How Obscurity-Based Privacy and a Right to Be Forgotten Are Incompatible with Free Speech*, 18 COMM. L. & POL'Y 91, 119–20 (2013) ("The concept of a privacy interest arising out of the obscurity of information . . . [is] fundamentally at odds with the established theories that undergird the American First Amendment right of freedom of speech.").

101. *See supra* note 100 and accompanying text (presenting doctrinal arguments against calls for a right to obscurity).

102. *See* Anderson, *supra* note 100, at 550 ("[T]hese scholars' demand for a right to obscurity is misplaced because they (i) overstate the potential harms linked to more technologically-advanced and democratized exposure, and (ii) inadequately account for the many benefits of exposure that would be blocked should their quest for a tight to obscurity succeed.").

the Supreme Court reached the wrong decision in *Los Angeles Police Department v. United Reporting Company*.[103] That case concerned a California statute that prevented people from receiving access to government records of arrestees if they were going to use the information for commercial purposes like selling products or services.[104] The supposed problem with this decision is that the discrimination imposes "unwarranted" expense on the barred groups, risks creating a false sense of security that a privacy problem has been solved, and erroneously crafts policy based on the form information is stored in, rather than the "nature of the information" itself.[105]

Yet despite such criticism, we propose that obscurity can be the key to unifying the diaspora of modern surveillance theory and policy because of its utility and broad applicability due to its fundamental reliance on transaction costs and probabilities. As we discuss below, it is easier to explain why certain surveillance is problematic when surveillance is understood as loss of obscurity. A focus on obscurity can accommodate multiple interests in reforming surveillance law, making consensus more likely.

IV. Obscurity Should Be at the Center of the Government Surveillance Debate

Diverse theories inform how the law regulates surveillance and how scholars determine which ideals and principles should guide surveillance law reform. Key components of leading theories can be rephrased into obscurity terms. We believe that talking about surveillance as a loss of obscurity can render both policy and contemporary conversation about surveillance less fragmented. By outlining a conceptual center of gravity that underlies and connects different surveillance theories, we aim to create a new

103. 528 U.S. 32 (1999); *see also* ALAN CHARLES RAUL, PRIVACY AND THE DIGITAL STATE: BALANCING PUBLIC INFORMATION AND PERSONAL PRIVACY 60 (2002) ("Imposing additional expense on particular businesses to acquire the same information that is available to other parties, like journalists or advocacy groups, seems unwarranted.").

104. *United Reporting*, 528 U.S. at 34–36.

105. *See* RAUL, *supra* note 103, at 60 ("Moreover, differential denial of public access to public information may lull government agencies into believing they have solved a problem.").

and useful vantage point for assessing how far surveillance creep extends and determining how best to address the expansion.[106] In this Part, we will use Fourth Amendment jurisprudence and Neil Richard's theory of intellectual privacy as exemplars of how embracing obscurity can improve the state of surveillance law and theory, respectively.

A. Obscurity and the Fourth Amendment

Although the Fourth Amendment is the *locus classicus* of juridical approaches to surveillance, debate rages over unanswered questions and conflicting interpretations.[107] According to Andrew Guthrie Ferguson, there are structural reasons why discord has come to plague views about protections and permissions: tension exists between principles articulated before the digital age began and the new opportunities for surveillance that innovation has made possible; a patchwork approach to resolving cases has resulted in "doctrinal gaps," rather than a unified paradigm of surveillance theory; the guiding analytic concepts, including "probable cause" and "reasonable expectation of privacy," are overdetermined and require inherently contestable judgment to operationalize; and dispute exists over what basic value (or values) the Fourth Amendment is supposed to safeguard.[108]

---

106. *See infra* Part IV.B (discussing the link between surveillance theory and obscurity).

107. *See* Andrew Guthrie Ferguson, *Personal Curtilage: Fourth Amendment Security in Public*, 55 WM. & MARY L. REV. 1283, 1305–06 (2014) ("Scholars have debated the textual meaning of its clauses as well as the core purpose of the Amendment." (citations omitted)).

108. *See id.*

> [T]he method of surveillance should be irrelevant, and the results of the surveillance are all that should matter in determining whether an individual's reasonable expectation of privacy has been infringed. Thus, in applying the *Katz* test, courts should look only to the characteristics of the item or information being observed—its location, its nature, and/or the actions taken by the defendant to conceal it.

(citing Ric Simmons, *From Katz to Kyllo, A Blueprint for Adapting the Fourth Amendment to Twenty-First Century Technologies*, 53 HASTINGS L.J. 1303, 1321–22 (2002)); Christopher Slobogin & Joseph E. Schumacher, *Reasonable Expectations of Privacy and Autonomy in Fourth Amendment Cases: An Empirical Look at "Understandings Recognized and Permitted by Society*," 42 DUKE L.J. 727,

732 (1993) (discussing the intrusiveness theory); Christopher Slobogin, *Let's Not Bury* Terry*: A Call for Rejuvenation of the Proportionality Principle*, 72 ST. JOHN'S L. REV. 1053, 1053 (1998) (claiming that the Terry principle needs to be rejuvenated because later case law is too vague); Christopher Slobogin, *The World Without a Fourth Amendment*, 39 UCLA L. REV. 1, 4 (1991) (providing an overview of how searches and seizures should be handled without the Fourth Amendment); Daniel J. Solove, *Fourth Amendment Pragmatism*, 51 B.C. L. REV. 1511, 1511 (2010) ("[T]he Fourth Amendment should provide protection whenever a problem of reasonable significance can be identified with a particular form of government information gathering."); Orin S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 HARV. L. REV. 476, 479 (2011)

> When changing technology or social practice makes evidence substantially harder for the government to obtain, the Supreme Court generally adopts lower Fourth Amendment protections for these new circumstances to help restore the status quo ante level of government power. On the other hand, when changing technology or social practice makes evidence substantially easier for the government to obtain, the Supreme Court often embraces higher protections to help restore the prior level of privacy protection.

James J. Tomkovicz, *Technology and the Threshold of the Fourth Amendment: A Tale of Two Futures*, 72 MISS. L.J. 317, 322–23 (2002)

> Official exploitation of a scientific or technological device should be considered a Fourth Amendment search at least when the effect is to enhance, augment or supplement human sensory abilities or other capacities in ways that have made it possible for the authorities to gain access to any information that otherwise would have been, or is highly likely to have been, imperceptible or inaccessible or would only have been, or is highly likely only to have been, perceived or acquired by means that are governed by the Fourth Amendment.

Christopher Slobogin, *Public Privacy: Camera Surveillance of Public Places and the Right to Anonymity*, 72 MISS. L.J. 213, 217 (2002)

> Continuous, repeated or recorded government surveillance of our innocent public activities that are not meant for public consumption is neither expected nor to be condoned, for it ignores the fundamental fact that we express private thoughts through conduct as well as through words. The Fourth Amendment should be construed to recognize the right to public anonymity as a part of the privacy expectations that, to use the Supreme Court's well-known phrase, "society is prepared to recognize as reasonable."

Raymond Shih Ray Ku, *The Founders' Privacy: The Fourth Amendment and the Power of Technological Surveillance*, 86 MINN. L. REV. 1325, 1326 (2002) ("The Fourth Amendment protects power not privacy."); Jeremy M. Miller, *Dignity as a New Framework, Replacing the Right to Privacy*, 30 T. JEFFERSON L. REV. 1, 20 (2007)

> For example, were "search" defined as a violation of intrinsic human dignity, it is likely the Court would recognize aerial surveillance into one's backyard, without warrant, as a violation of the home dweller's dignity. Stop and frisk, based on less than probable cause, would similarly violate reasonable standards of dignity. And, for the motorist,

Perhaps the most important recent case to cause controversy over how to interpret the Fourth Amendment is *United States v. Jones*.[109] There, the Justices unanimously ruled that police performed a constitutionally prohibited search when, one day after their warrant expired, they installed a GPS device to a car's undercarriage that suspected narcotics dealer Antoine Jones drove with the intent of keeping tabs on his activity.[110] For twenty-eight days, the government unrelentingly tracked and recorded where the vehicle went, amassing over 2,000 pages of location data.[111]

The majority opinion focused on the act of physical intrusion that had transpired.[112] But concurring opinions from Justices Sotomayor and Alito clarified why this narrow approach leaves deep problems on the horizon.[113] Eighteenth-century trespass law rooted in property-rights theory might suffice to resolve the matter

---

> whose car might in fact be his or her most cherished place, arbitrary police intrusion might preclude much that happens today, since under present law, if one steps into his or her car, he or she surrenders the "right to be let alone."

Andrew E. Taslitz, *The Fourth Amendment in the Twenty-First Century: Technology, Privacy, and Human Emotions*, 65 LAW & CONTEMP. PROBS. 125, 169 (2002)

> Privacy is, however, more a matter of affect than cognition. Privacy is a set of metaphorical boundaries that enables each of us to safeguard a sense of self. Privacy enables us to decide which aspects of ourselves to reveal and to whom. That control matters deeply, because overly selective exposure of ourselves to others will lead to their misjudging our nature.

Andrew E. Taslitz, *Respect and the Fourth Amendment*, 94 J. CRIM. L. & CRIMINOLOGY 15, 98 (2003) ("The Fourth Amendment protects core interests essential to human flourishing, interests in privacy, property, and freedom of movement."); Scott E. Sundby, *"Everyman's" Fourth Amendment: Privacy or Mutual Trust Between Government and Citizen?*, 94 COLUM. L. REV. 1751, 1775 (1994) (claiming that government surveillance has reduced "the right to be left alone").

109. 132 S. Ct. 945 (2011).

110. *See id.* at 948 (explaining that the government used the tracking device for twenty-eight days).

111. *See id.* (charging the defendant based on the information obtained from the tracking device).

112. *See id.* at 949–52 (explaining that the *Katz* reasonable expectation of privacy test did not replace the Fourth Amendment trespassory test).

113. *See id.* at 954–64 ("[B]ecause GPS monitoring is cheap in comparison to conventional surveillance techniques and, by design, proceeds surreptitiously, it evades the ordinary checks that constrain abusive law enforcement practices . . . .").

at hand, given the contingent circumstances involved, but it is inadequate for resolving the broader twenty-first century privacy problems that occur when the use of powerful and ubiquitous surveillance technologies clash with the privacy interests people often claim to have while being in public.[114] Simply put, while the Court ruled that Jones's Fourth Amendment rights were violated, it did not clarify whether warrantless surveillance that yields the type of scrutiny Jones was subjected to—consider, for example, the possibility of the government monitoring smart phone GPS coordinates—should be deemed unreasonable, in principle, under the Fourth Amendment.[115]

While Justices Alito and Sotomayor did not explicitly adopt obscurity terminology, their remarks clearly convey appreciation for the logic of obscurity theory. Indeed, they essentially frame lingering privacy concerns as obscurity issues, and in so doing hint at the radical possibility that the Fourth Amendment stands to lose much of its social value if its interpretation fails to better address the problems that obscurity theory renders salient.

Justice Sotomayor stated that "it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties."[116] She further maintained that she "would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection."[117] We see this as a clear appeal to consider additional constitutional protections for obscurity interests—to acknowledge that when citizens communicate with select audiences, it may still be reasonable for them to expect protections from forms of surveillance that bring heightened publicity to their disclosures.

Justice Sotomayor suggests that such protections are especially relevant to consider in cases where the government

---

114. *See id.* at 956 ("Awareness that the Government may be watching chills associational and expressive freedoms.").

115. *See id.* at 955 (explaining that physical intrusion is no longer necessary for surveillance in many instances).

116. *See id.* at 956–57 (noting that the premise "is ill suited to the digital age").

117. *See id.* at 957 (emphasizing that she believes telling a third party information for a limited use does not erase the person's expectation of privacy).

easily can use efficient aggregation technology to transform otherwise discrete and comparatively obscure forms of information into integrated portraits that are conveniently available in a single location. Clear pictures of patterned behavior impinge on privacy interests because they can reveal intimate dispositions and preferences. Accordingly, Justice Sotomayor writes:

> I would take these attributes of GPS monitoring into account when considering the existence of a reasonable societal expectation of privacy in the sum of one's public movements. I would ask whether people reasonably expect that their movements will be recorded and aggregated in a manner that enables the Government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on.[118]

Justice Alito's remarks about long-term surveillance undermining privacy protections echo two of the views that we highlighted in Part III of this Article: Harper's historical sense of how privacy expectations developed alongside the practical limits that transaction costs impose and Surden's view of structural rights.[119] Regarding Harper's concerns of practical limitations, Justice Alito contends that "[i]n the pre-computer age, the greatest protections of privacy were neither constitutional nor statutory, but practical. Traditional surveillance for any extended period of time was difficult and costly and therefore rarely undertaken."[120] Regarding Surden's theory of structural protections, he claims that "society's expectation has been that law enforcement agents and others would not—and indeed, in the main, simply could not—secretly monitor and catalogue every single movement of an individual's car for a very long period."[121]

Both Justice Sotomayor and Justice Alito espouse ideas associated with what many have referred to as the "mosaic theory" of surveillance, which came to prominence in the case *United States v. Maynard*.[122] Orin Kerr has summarized the theory as requiring "courts to apply the Fourth Amendment search doctrine to government conduct as a collective whole rather than in isolated

---

118. *Id.*

119. *See supra* Part III (providing background on the obscurity theory).

120. United States v. Jones, 132 S. Ct. 945, 963 (2011).

121. *See id*. at 964 (highlighting the practical implications of the holding).

122. 615 F.3d 544 (D.C. Cir. 2010).

steps."[123] Kerr clarifies that "[i]nstead of asking if a particular act is a search, the mosaic theory asks whether a series of acts that are not searches in isolation amount to searches when conducted in a group."[124] A hypothetical application of mosaic theory, therefore, would be allowing government agents to engage in warrantless GPS tracking for a delimited period of time, but insisting that they obtain a warrant to continue on past this point.

Kerr acknowledges that legitimate concerns for "equilibrium-adjustment" motivate mosaic theory.[125] But he squarely recommends that the courts reject the mosaic theory, which he categorized as a "major departure" from traditional, sequential interpretations of what constitutes a search under the Fourth Amendment.[126] According to Kerr, if the courts were to make the mistake of adopting mosaic theory, they would need to solve highly complex and overly burdensome puzzles, such as setting appropriate standards for determining when a mosaic is completed and determining which approaches to data aggregation fall under the mosaic purview.[127]

Kerr is a leading critic of mosaic theory, but not everyone shares his pessimism about the costs of embracing it.[128] After all, if technology can eviscerate obscurity, perhaps it also can be used as a tool to pinpoint when too much obscurity evisceration takes place. In this spirit, Steven Bellovin, Renée Hutchins, Tony Jebara, and Sebastian Zimmeck have contended that advances in the computer-science approach to machine learning make it possible in some domains to determine when an agreed upon

---

123. *See* Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311, 320 (2012) [hereinafter *Mosaic Theory*] (meaning that together the events can constitute a search even if the individual steps do not).

124. *See id.* (explaining the mechanics of the mosaic theory).

125. *See* Orin S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 HARV. L. REV. 476, 479–82 (2012) (elaborating more fully on what equilibrium-adjustment is and why he believes it should be defended).

126. *See Mosaic Theory*, *supra* note 123, at 314–15 (highlighting how the mosaic theory is disjointed from traditional case law).

127. *See id*. at 314 (emphasizing the practical concerns associated with the mosaic theory).

128. *See, e.g.*, Steven Bellovin, Renée Hutchins, Tony Jebara & Sebastian Zimmeck, *When Enough is Enough: Location Tracking, Mosaic Theory, and Machine Learning*, 8 NYU J.L. & LIBERTY 556, 556–628 (2014) (supporting the mosaic theory).

threshold of overly invasive search has been breached.[129] Under current algorithmic constraints, they argue that an approximate tipping point can be specified for going too far for warrantless geo-location tracking.[130] The demarcation, they speculate, is exceeding a week.[131]

Jones is just one example of how obscurity is already embedded as a concept in surveillance law, yet courts have not adequately conceptualized it. This leads to splintered theories regarding theories of duration, information sensitivity, and trespass with no real locus for moving forward. By focusing on obscurity and transaction costs, courts would be able to isolate the operative factors concerning when an expectation of privacy is reasonable and a search is thus unreasonable.

B. Obscurity and Surveillance Theory

In addition to courts and policy-makers, surveillance theorists can also benefit from appeals to obscurity. To say that something is obscure is to describe it. As a descriptive concept, obscurity can be utilized by other theories of surveillance to explain when and why surveillance is problematic. In this way, obscurity can serve as a common thread for surveillance theorists. In this Part, we will demonstrate how the language of obscurity can supplement privacy theory by exploring, among other theories, the intersection between obscurity and the concept of "intellectual privacy" that Neil Richards developed.[132]

Richards draws the line against government and corporate surveillance when agents, agencies, and corporations intrude too deeply upon "intellectual privacy"—the right for citizens in a free society to be granted a great deal of latitude to learn and express themselves without experiencing the behavior-altering chill that

129. *See id*. (focusing on the importance of the use of technological advances on the benefits of the mosaic theory).

130. *See id*. (providing an example of how the technology could be utilized).

131. *See id.* at 625 (explaining the use of data sets in more detail).

132. *See generally* NEIL RICHARDS, INTELLECTUAL PRIVACY: RETHINKING CIVIL LIBERTIES IN THE DIGITAL AGE (2015) (discussing the complexities of corporate and government surveillance and the freedom of speech).

comes from suspecting intimate, belief-forming, and belief-sharing activities are being monitored, such as reading and debating.[133]

A pressing challenge for intellectual privacy is the diminishing obscurity of public activity. Although public places are readily associated with heightened expectations of visibility, the fact remains that people engage with controversial ideas that expand their political and moral imaginations in public places all the time because they anticipate that what they say and do will only be observed by limited, local audiences.[134] In other words, people routinely speak their minds publicly without presupposing that they are entering into full-blown public debate.[135] They even view exchanges occurring in public as preparatory work for acquiring the psychological confidence and justificatory arguments needed to subsequently offer interesting remarks for more of the general public to consider. These behaviors and attitudes exist because free-flowing social interaction is a crucial component of developing and maintaining a mature and responsible consciousness.

There is ample evidence that Richards's view of intellectual privacy is widely maintained, even though the average person does not use such technical vocabulary to describe why it is possible to leave the house without becoming paranoid. For example, when people dine at restaurants, they are willing to engage in passionate arguments about contentious subjects rather than fearfully sticking to bland topics, like the weather. Folks are also comfortable marching in parades for social causes they are committed to, but do not necessarily want everyone who knows them to be aware of the cause they support. People are often even okay consuming media about unpopular and risqué topics while travelling on public transportation and sitting at cafes. But these attitudes can change. Surveillance technologies that dramatically minimize the transaction costs required for others to record and share information featuring or about us performing these and related activities can undermine our willingness to pursue them. According to Richards, such a blow to what we call obscurity would be potent enough to damage the fabric of democracy.[136]

---

133. *See id*. at 5 (emphasizing the problems of intellectual privacy).

134. *Id*. at 157.

135. *Id*.

136. *See id*. at 3 ("[W]e need to be clearer by what we mean by both 'privacy'

Another reason that the right to intellectual privacy is important in the digital age is that so much of what we disclose and peruse occurs over media connected to the Internet. Richards and others thus express concern over technologies that promote so-called "frictionless" modes of social reading that minimize the control we can exert over what companies and other people know about our literary habits.[137] "Under current law," Richards writes, the electronic commerce company Amazon.com "is free to sell all of its sensitive data however it wants to."[138] This discretionary latitude is disconcerting because, by default, Amazon's popular e-reader, the Kindle, "keeps detailed records of what we buy, browse, how long our mouse rests over a word and our eyes linger over a page, what pages we underline and what the most underlined pages are, whether we finish a book, whether we re-read a book, and what passages we re-read."[139] By emphasizing technologically induced, diminished transaction costs, Richards again effectively identifies decreased obscurity as the root of problematic surveillance.[140]

Obscurity problems are also related to Richards's worries that government surveillance is endangering intellectual privacy.[141] Consider, for example, his stance on the encryption debate that was going strong during the fall of 2014 and which persisted well

---

and 'speech.' We need to think more deeply about the complexity of these two values, what they mean, what they do for us, and the surprising, mutually reinforcing relationships between them.")

137. *See* Neil Richards, *The Perils of Social Reading*, 101 GEO. L.J. 689, 690–724 (2013) (warning about the information individuals give to corporations and their loss of control over the information); William McGeveran, *The Law of Friction*, U. CHI. L. REV. 15, 15 (2013) (noting that frictionless sharing discloses individual's data immediately).

138. *See* Evan Selinger, *What Is Intellectual Property, and How Yours Is Being Violated*, CHRISTIAN SCI. MONITOR (Feb. 25, 2015), http://www.csmonitor.com/World/Passcode/Passcode-Voices/2015/0225/What-is-intellectual-privacy-and-how-yours-is-being-violated (last visited June 18, 2015) (claiming that there are real political ramifications stemming from our intellectual data) (on file with the Washington and Lee Law Review).

139. *See id*. (focusing on the fact that librarians have ethical confidentiality obligations, but corporations like Kindle do not).

140. *See id*. (acknowledging that one avenue this problem shows up in is internet advertising).

141. *See id*. (explaining that intellectual privacy affects everyone—not just the scholars).

into the following year.[142] Companies like Apple offered consumers products with strong encryption: the iOS 8 operating system, for example, provides encryption by default, and this means that the data stored on up-to-date iPhones cannot be accessed without breaking this encryption—an act that requires using the owner's password or key.[143] Security experts like Kevin Poulsen depicted manufacturing and distributing these products as gestures that distance Silicon Valley companies from being branded as "NSA collaborators."[144] But President Obama was so dismayed over the absence of backdoors that he decried designs that lock out government agents.[145]

Richards is not persuaded by the logic of the President's opposition.[146] Appealing to intellectual privacy, Richards states, "Encryption provides necessary safeguards by securing what we're thinking until we're ready to enter public debate."[147] When pressed further about why due process does not assuage his worries about how the government will use backdoors, Richards justifies his position by stating that civil rights are protected when transaction costs prevent the government from conducting over-zealous

---

142. *See* Editorial Board, *Compromise Needed on Smart Phone Encryption*, WASH. POST (Oct. 3, 2014), http://www.washingtonpost.com/opinions/compromise-needed-on-smartphone-encryption/2014/10/03/96680bf8-4a77-11e4-891d-713f052086a0_story.html (last visited June 18, 2015) (analyzing the link between technology, legal, and privacy concerns) (on file with the Washington and Lee Law Review).

143. *See id*. (explaining that the encryption is so strong Apple cannot even break it for law enforcement).

144. *See* Kevin Poulsen, *Apple's iPhone Encryption is a Godsend, Even if Cops Hate It*, WIRED (Oct. 8, 2014, 6:30 A.M.), http://www.wired.com/ 2014/10/golden-key/ (last visited June 18, 2015) (explaining that several large corporations were painted as "NSA Collaborators" by Edward Snowden) (on file with the Washington and Lee Law Review).

145. *See id*. ("With the release of iOS 8, Apple made a privacy improvement so dramatic that it should rightly wipe out the taint of these security failures. Instead, the company is bashed by the nation's top law enforcement official and the editorial board of one of the country's most prestigious newspapers."); *see also* Danny Yadron, *Obama Sides with Cameron in Encryption Fight*, WALL ST. J. (Jan. 16, 2015, 4:52 PM), http://blogs.wsj.com/digits/2015/01/16/obama-sides-with-cameron-in-encryption-fight/ (last visited June 18, 2015) (discussing President Obama's stance on spy access to encrypted cell phones) (on file with the Washington and Lee School of Law).

146. *See* Selinger, *supra* note 138 (explaining the strength of encryption compared to frictionless information sources).

147. *Id*.

searches.[148] Although, yet again, he does not make an explicit appeal to obscurity, the proffered argument presupposes the causal logic that lies at the heart of obscurity theory:

> We know from Snowden and others that very often due process in national security cases is minimal to non-existent, and better checks need to be in place than the ones we currently have. Also, encryption doesn't mean that government can't ever get access to information, any more than putting locks on a door means that nobody can break into a house. The government's response to this retort is that encryption makes it harder for law enforcement to do its job. But that's exactly the point of civil liberties like intellectual privacy. They introduce inefficiencies.[149]

When Richards emphasizes that the government can still access data that a citizen has stored on his or phone even without a back door, he is referring to the range of legal options available.[150] For example, if the government is looking for e-mail, it can approach a service provider and follow the routes permitted under the ECPA; depending on factors like date and whether an e-mail has been opened, the possibilities range from obtaining a warrant, obtaining a subpoena and sending out notification, or simply obtaining a court order. Or, if the desired information is stored in the cloud (for example, in places like Google Drive or Dropbox), the government typically can get its way with only a court order. And while consensus does not exist about whether a warrant is sufficient to compel an individual to decrypt a device, that outcome has arisen in cases like *United States v. Fricosu*[151] and *Commonwealth v. Gelfgatt*.[152]

This is not the first time Richards has called for limiting government surveillance by changing obscurity dynamics through the introduction of practical inefficiencies.[153] In 2013, he argued:

---

148. *See id.* at 717 (explaining that confidential rules should guide disclosures of sensitive information).

149. *Id.*

150. *See id.* (noting also that backdoors make it easier for malicious hackers to access as well).

151. 841 F. Supp. 2d 1232 (D. Colo. 2012).

152. *See* 468 Mass. 512 (2014) (dealing with a forgery that involved encryption).

153. *See* Neil Richards, *Don't Let U.S. Government Read Your E-mail*, CNN (Aug. 18, 2013 9:04 AM ET), http://www.cnn.com/2013/08/18/opinion/richards-

> We should presume the privacy of e-mail and other communications, and we should require the government to get warrants supported by probable cause before it can read our mail, track our movements and use our communications data to construct a map of everyone we know and when we talk to them.[154]

In this context, Richards laments that Lavabit and Silent Circle, companies that provided encrypted and secure e-mail services, were essentially forced to shut down due to government pressure.[155] Such disappointment can be described in obscurity terms, as Stefanie Pell's work demonstrates.[156]

When Pell discusses Silent Circle, she insists that the technology and others like it can play a special role in our post-*United States v. Jones* society.[157] The essence of her argument is that because it appears likely that time will need to pass before legislation is created that is in line with the concurring opinions of the Justices who are sympathetic to interpreting the Fourth Amendment in terms that reflect the mosaic theory, the power of code to function as what Lawrence Lessig calls a "regulator" should not be underestimated.[158] Accordingly, she writes:

> While waiting for more definitive action from the courts and Congress, such "privacy enhancing" anonymization and encryption technologies can provide a temporary "fix" to the problem of ever-expanding police powers in the digital age, insofar as they make law enforcement investigations more difficult and expensive, thereby forcing law enforcement to prioritize some investigations and, perhaps, deemphasize or drop others.[159]

---

lavabit-surveillance/ (last visited June 19, 2015) (emphasizing that communication is at the heart of our political freedoms) (on file with the Washington and Lee Law Review).

154. *Id*.

155. *See id*. (explaining that the government was pressuring them to hand over Edward Snowden's records).

156. *See generally* Stefanie Pell, *Jonesing for a Privacy Mandate, Getting a Technology Fix—Doctrine to Follow*, 14 N.C. J. L. & TECH. 489 (2013).

157. *See id*. at 531 (explaining that Silent Circle is an encryption service offering encrypted texts and phone calls).

158. *See id*. at 489 (providing an overview of her article).

159. *Id*.

Obscurity can also aid theories that describe why dragnet surveillance involving large quantities of information is dangerous. Because most of our lives are lived in obscurity, the specter of surveillance occurring "most of the time" threatens to jeopardize this important default—a state of affairs that protects people from having to scrutinize every move they make. In the big data age, where digital dossiers containing massive amounts of personal data are expanding at an alarming rate, an appeal to obscurity can provide support for what David Gray and Danielle Citron call a right to "quantitative privacy."[160]

Gray and Citron begin their account of quantitative privacy by looking to the concurrences in *United States v. Jones*.[161] They note that "[t]hose Justices insisted that citizens possess a Fourth Amendment right to expect that certain quantities of information about them will remain private, even if they have no such expectations with respect to any of the discrete particulars of that information."[162] Under this theory, "even if the use of a GPS-enabled tracking device to effect 'relatively short-term monitoring of a person's movements on public streets' does not implicate the Fourth Amendment, 'the use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy.'"[163]

The scholars note this is a revolutionary theory with an unclear fit in standard Fourth Amendment pedigree.[164] According to Gray and Citron, "[a] quantitative approach to the Fourth Amendment appears to undercut well-established rules, including

---

160. *See generally* David C. Gray & Danielle Keats Citron, *A Technology-Centered Approach to Quantitative Privacy* (2012) [hereinafter *Quantitative Privacy*], *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id= 2129439; *see also* David C. Gray & Danielle Keats Citron, *The Right to Quantitative Privacy*, 98 MINN. L. REV. 62, 71 (2013) [hereinafter *Right to Quantitative Privacy*] (discussing quantitative privacy and the mosaic theory's dominance).

161. *See Quantitative Privacy*, *supra* note 160, at 12 (discussing Justice Sotomayor's opinion).

162. *See id.* at 68 (highlighting the difference between short term and long term surveillance).

163. *Id.*

164. *See id.* (claiming that it undercuts current doctrine, including third-party rules).

the public observation doctrine and the third-party doctrine."[165] They note the theory's challenges, stating

> Defenders of quantitative privacy must chart a conceptual link to these precedents or provide compelling reasons for changing course. Advocates also must provide a workable test that law enforcement and courts can employ in drawing the line between quantities of data that do and do not trigger the Fourth Amendment.[166]

The scholars propose a theory to do just that, stating, "Rather than asking how much information is gathered in a particular case, we argue here that Fourth Amendment interests in quantitative privacy demand that we focus on how information is gathered."[167] Gray and Citron argue that:

> [T]he threshold Fourth Amendment question should be whether a technology has the capacity to facilitate broad and indiscriminate surveillance that intrudes upon reasonable expectations of quantitative privacy by raising the specter of a surveillance state if deployment and use of that technology is left to the unfettered discretion of law enforcement officers or other government agents.[168]

Note that this theory is, at base, reliant upon the notion of transaction costs for surveillance. High transaction costs for surveillance eliminate the specter of a surveillance state because it would be resource intensive. Gray and Citron explicitly recognize this, stating that factors to consider when determining the capacity for broad, indiscriminate surveillance include "(1) the inherent scope of a technology's surveillance capabilities, be they narrow or broad; (2) the technology's scale and scalability; and (3) the costs

---

165. *Id.*

166. *Id.*

167. *Id.* at 71.

168. *See id.* at 71–72

> If it does not, then the Fourth Amendment imposes no limitations on law enforcement's use of that technology, regardless of how much information officers gather against a particular target in a particular case. By contrast, if it does threaten reasonable expectations of quantitative privacy, then the government's use of that technology amounts to a "search," and must be subjected to the crucible of Fourth Amendment reasonableness, including judicially enforced constraints on law enforcement's discretion.

associated with deploying and using the technology."[169] Looking at these factors,

> [i]f a court finds that a challenged technology is capable of broad and indiscriminate surveillance by its nature, or is sufficiently inexpensive and scalable so as to present no practical barrier against its broad and indiscriminate use, then granting law enforcement unfettered access to that technology would violate reasonable expectations of quantitative privacy.[170]

One way to articulate when the right to quantitative privacy is threatened is when the obscurity is lost. When transaction costs fall, large amounts of previously obscure information are surveilled. Obscurity explains *when* and *why* quantitative privacy is triggered. Bulk quantities of information are important to protect, not because they are sensitive, but because people relied upon the obscurity of this, and indeed most, information. Gray and Citron even explicitly acknowledge the relationship between practical obscurity and quantitative privacy when they discuss the *Reporter's Committee* opinion.[171]

According to the scholars that developed the theories, quantitative privacy is distinct from intellectual privacy with respect to surveillance. In a response to Neil Richards's article *The Dangers of Surveillance*,[172] which articulated a theory of intellectual privacy for surveillance, Gray and Citron argue, "although Richards aptly captures the dangers to intellectual freedom posed by technologically enhanced surveillance, we fear his policy prescriptions are both too narrow and too broad because they focus on 'intellectual activities' as a necessary trigger and metric for judicial scrutiny of surveillance technologies."[173] According to Citron and Gray, "by focusing too much on what information is gathered rather than how it is gathered, efforts to

---

169. *See id.* at 102 (highlighting the high transactions costs associated with surveillance).

170. *Id.*

171. *See id.* at 113–14 (mentioning that the costs of mass surveillance has been dramatically reduced).

172. Neil Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. F. 1934 (2013).

173. Danielle Citron and David Gray, *Addressing the Harm of Total Surveillance: A Reply to Professor Neil Richards*, 126 HARV. L. REV. F. 262, 266 (2013).

protect reasonable expectations of privacy threatened by new and developing surveillance technologies will disserve the legitimate interests of both information aggregators and their subjects."[174]

They continue, "One reason we are troubled by Richards's focus on 'intellectual activities' as the primary trigger for regulating surveillance technology is that it dooms us to contests over which kinds of conduct, experiences, and spaces implicate intellectual engagement and which do not."[175] Gray and Citron propose an alternative: "Rather than assigning primary importance to 'intellectual activities' and presumably providing less protection against the acknowledged perils of broader types of surveillance, the law's focus should be on the dangers of totalizing surveillance."[176]

The concept of obscurity is thus useful for narrowing the gap between intellectual privacy and quantitative privacy theories. By recognizing that remedies focusing on transaction costs and preserving the obscurity of information can simultaneously foster intellectual privacy and quantitative privacy, it becomes easier to appreciate the common ground that Richards, Citron, and Gray share.[177] Not only can policy recommendations build upon this commonality to create outcomes that both theories would validate as just (albeit for different reasons), but it also becomes possible to see how the type of machine-learning research championed by Steven Bellovin, Renée Hutchins, Tony Jebara, and Sebastian Zimmeck has the potential to advance outcomes prized by both theories too.[178] Quantitative insights can illuminate when aggregation covers sufficient ground as to minimize the obscurity necessary for maintaining intellectual privacy and avoiding the threshold wherein indiscriminate surveillance occurs.

---

174. *Id.* at 267.

175. *Id.*

176. *See id.* at 270 ("The threat posed by contemporary surveillance technologies lies in how much and how often people are watched.").

177. *See generally* Richards, *supra* note 132; *Quantitative Privacy*, *supra* note 160.

178. *See generally* Bellovin, *supra* note 128.

V. Conclusion

When government surveillance is understood as a series of discrete problems that just happen to be occurring at the same time, conceptual bias hinders surveillance reform: the right approach for finding solutions appears to be proposing discrete remedies. The patchwork approach to U.S. privacy law and judicial concern about undue activist overreach entrenches this propensity. The fragmentation of surveillance law further limits many proposed surveillance protections to conservative gestures based on doctrines whose applicability is increasingly challenged by powerful and cheaply available technology that disrupts social and institutional norms.

Once it is clear that a common theoretical center of gravity underlies diverse surveillance problems and claims about why surveillance creep needs to be reined in, it becomes less challenging to imagine far-reaching and holistic approaches to progress. In this Article, we have argued that framing surveillance dilemmas as obscurity predicaments is a crucial step towards that goal.

Applying obscurity theory's two principle insights—the behavior-altering power of transaction costs and sociological explanation of why reasonable expectations for privacy can exist for public disclosures—is the key for identifying significant, common themes that have been communicated across forward-looking surveillance literatures. The main conclusion that can be drawn under a unified obscurity-based approach to surveillance is that a *democratically accountable government should find it appropriately difficult to violate the privacy rights of its citizens*.

Of course, determining what the threshold should be for calibrating appropriate difficulty is a contentious normative endeavor. No analyst can determine it solely by appealing to obscurity theory; after all, the framework is inherently descriptive. Nevertheless, it would be a mistake to underestimate the explanatory value of seeing *undue expediency in obtaining or interpreting information as the fundamental problem plaguing government surveillance*. Keeping this issue in mind when analyzing the specifics involved with any particular surveillance case makes it easier to appreciate why pervasive surveillance anxiety exists, how that anxiety can magnify the practical stakes

involved in a given instance, and why seemingly unrelated options for further justice (ranging from requiring warrants to proposing measures that make it harder to aggregate mosaics) actually converge around a common objective: adding friction into a process or system to make a person or piece of information harder to find or understand, thus preserving obscurity.