3-2019

The Public Information Fallacy

Woodrow Hartzog
Boston University School of Law

THE PUBLIC INFORMATION FALLACY

WOODROW HARTZOG[*]

ABSTRACT

The concept of privacy in "public" information or acts is a perennial topic for debate. It has given privacy law fits. People struggle to reconcile with traditional accounts of privacy the notion of protecting information that has been made public. As a result, successfully labeling information as public often functions as a permission slip for surveillance and personal data practices. This label has also led to a significant and persistent misconception—that public information is an established and objective concept.

In this Article, I argue that the "no privacy in public" justification is misguided because nobody knows what "public" means. It has no set definition in law or policy. Appeals to the public nature of information in order to justify data and surveillance practices is often just guesswork. There are at least three different ways to conceptualize public information: descriptively, negatively, or by designation. For example, is the criterion for determining publicness whether it can be described as hypothetically accessible to anyone? Or is public information anything that is controlled, designated, and released by state actors? Or maybe what is public is simply everything that is "not private"?

If the concept of "public" is going to shape people's social and legal obligations, we ought not to assume its meaning. Law and society must recognize that labeling something as public is both consequential and value-laden. To move forward, we should focus on the values we want to serve, the relationships and outcomes we want to foster, and the problems we want to avoid.

[*] Professor of Law and Computer Science, Northeastern University School of Law and College of Khoury Computer Sciences; Affiliate Scholar, The Center for Internet and Society at Stanford Law School. The author wishes to thank Jack Balkin, Victoria Baranetsky, Jeff Brueggeman, Rebecca Crootof, Brannon Denning, Chris Hoofnagle, Margot Kaminski, William McGeveran, Neil Richards. Paul Schwartz, Evan Selinger, Scott Skinner-Thompson, and Daniel Solove. This Article benefitted temendously from input by participants at the Amsterdam Privacy Confernce, the Future of Privacy Forum's Privacy Papers for Policy Makers event, the Privacy Law Scholars Conference, and the Yale Information Society Project's Ideas Lunch. I also wish to thank Siri Nelson for her great research assistance.

CONTENTS

INTRODUCTION

Sometimes the way we discuss, and regulate, privacy feels a little delusional. We "agree" to privacy policies. We are promised "control" over our personal information. Unless our identities or money are stolen, computer hacks do not seem to register as "harmful" to us. But one of the most overlooked misconceptions lawmakers and society often labor under is that "public" information is an established and objective concept.[1] One of the most reliable permission slips for surveillance and data practices in the United States is successfully claiming that the information at issue was "public" or that the person surveilled was "in public."[2]

Judges considering privacy tort claims have said for years that "there can be no privacy in that which is already public."[3] They littered their opinions with statements like "[u]sers would logically lack a legitimate expectation of privacy in the materials intended for publication or public posting."[4] The FBI alleges it does not need permission to conduct surveillance using powerful technologies

[1] *See, e.g.*, John Lawrence Hill, *The Constitutional Status of Morals Legislation*, 98 KY. L.J. 1, 17 (2009) (discussing scope of right to privacy under the Constitution and finding that "there is no purely objective concept of harm to which we can appeal to tell us where to draw the line between the private and public realms").

[2] *See* Gill v. Hearst Publ'g Co., 253 P.2d 441, 444-45 (Cal. 1953) ("The photograph of plaintiffs merely permitted other members of the public, who were not at plaintiffs' place of business at the time it was taken, to see them as they had voluntarily exhibited themselves. Consistent with their own voluntary assumption of this particular pose in a public place, plaintiffs' right to privacy as to this photographed incident ceased and it in effect became a part of the public domain . . . . In short, the photograph did not disclose anything which until then had been private, but rather only extended knowledge of the particular incident to a somewhat larger public than had actually witnessed it at the time of occurrence." (citations omitted)); Moreno v. Hanford Sentinel, Inc., 91 Cal. Rptr. 3d 858, 862-63 (Ct. App. 2009) ("Here, Cynthia publicized her opinions about Coalinga by posting the Ode on myspace.com, a hugely popular internet site. Cynthia's affirmative act made her article available to any person with a computer and thus opened it to the public eye. Under these circumstances, no reasonable person would have had an expectation of privacy regarding the published material. . . . There is no allegation that Campbell obtained Cynthia's identification from a private source. In fact, Cynthia's MySpace page included her picture. Thus, Cynthia's identity as the author of the Ode was public. In disclosing Cynthia's last name, Campbell was merely giving further publicity to already public information. Such disclosure does not provide a basis for the tort.").

[3] *See, e.g.*, *Gill*, 253 P.2d at 444.

[4] Guest v. Leis, 255 F.3d 325, 333 (6th Cir. 2001); *see also* United States v. Maxwell, 45 M.J. 406, 419 (C.A.A.F. 1996) ("Messages sent to the *public at large* in the 'chat room' or e-mail that is 'forwarded' from correspondent to correspondent lose any semblance of privacy." (emphasis added)); Dexter v. Dexter, No. 2006-P-0051, 2007 WL 1532084, at *6 n.4 (Ohio Ct. App. May 25, 2007) ("[W]ith respect to her Myspace account, appellant admitted in open court that she wrote these on-line blogs and that these writings were *open to the public to view*. Thus, she can hardly claim an expectation of privacy regarding these writings." (emphasis added)).

like cell-site simulators (often called "Stingrays"), so long as they are doing so in public places.[5] Judges have refused to punish people for taking "upskirt" photos because the women photographed have no reasonable expectation of privacy "in public," no matter how fleeting their exposure.[6] And those are just a few examples.

The concept of "public information and acts" is entrenched in U.S. law and policy. Tort law, statutes, and interpretations of constitutional amendments regularly deploy the concept of "public information" to justify surveillance or data practices.[7] The Securities and Exchange Commission ("SEC") does not consider buying or selling securities on the basis of public information insider

[5] David Kravets, *FBI Says Search Warrants Not Needed to Use "Stingrays" in Public Places*, ARS TECHNICA (Jan. 5, 2015, 2:25 PM), https://arstechnica.com/tech-policy/2015/01/fbi-says-search-warrants-not-needed-to-use-stringrays-in-public-places/ [https://perma.cc/J5JE-U29B] (discussing FBI's position that court warrants are not required when collecting cell-site data in public places); David Kravets, *Feds: Privacy Does Not Exist in 'Public Places,'* WIRED (Sept. 21, 2010, 3:29 PM), https://www.wired.com/2010/09/ public-privacy/ (discussing FBI's argument that tracking public movements of suspect's vehicle through GPS devices does not require warrant); Press Release, Chuck Grassley, U.S. Senator, Leahy & Grassley Press Administration on Use of Cell Phone Tracking Program (Dec. 31, 2014), https://www.grassley.senate.gov/news/news-releases/leahy-grassley-press-administration-use-cell-phone-tracking-program [https://perma.cc/4PQL-H2GD] (arguing that scope of FBI ability to acquire information through cell-site simulators without warrant is overly broad).

[6] *See, e.g.*, Order to Suppress Physical Evidence and Statements at 2-3, United States v. Cleveland, No. 10-DVM 1341 (D.C. Super. Ct. 2014) ("[T]he issue is more accurately defined as whether women in a public place with private areas of their body exposed to public view have a reasonable expectation of privacy . . . . 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 other individuals could have a reasonable expectation of privacy.").

[7] *See, e.g.*, Florida v. Jardines, 133 S. Ct. 1409, 1414 (2013) (limiting Fourth Amendment protection of privacy in home to area "immediately surrounding" home); Illinois v. Caballes, 543 U.S. 405, 409-10 (2005) (finding drug dog brought to outside of defendant's car does not violate privacy rights because "[t]he legitimate expectation that information about perfectly lawful activity will remain private is categorically distinguishable from respondent's hopes or expectations concerning the nondetection of contraband in the trunk of his car"); California v. Ciraolo, 476 U.S. 207, 212-14 (1986) (finding defendant did not have privacy violated when police officers spotted marijuana growing in defendant's backyard from airplane); United States v. Jacobsen, 466 U.S. 109, 118-22 (1984) (refusing to extend privacy right to protect package that had already been searched by Federal Express employee and contained white powder not directly visible because officials were operating with information from a third party); United States v. Place, 462 U.S. 696, 706-07 (1983) (holding that when "officer's observations lead him reasonably to believe that a traveler is carrying luggage that contains narcotics" there is no violation of defendant's privacy rights if officer uses drug sniffing dog); Smith v. Maryland, 442 U.S. 735, 744-46 (1979) (finding no privacy right to information willingly conveyed through telephone records); United States v. Miller, 425 U.S. 435, 442-43 (1976) (refusing to extend privacy protection to checks given to bank).

trading.[8] The U.S. Department of Health and Human Services ("HHS") even briefly considered excluding "public" data sets from research oversight because, in its view, doing so presents a low risk of harm.[9] Law and society regularly endow the concept of "public information" with great power while at the same time uncritically accepting the concept as a tenet of faith. It is as though the concept is invoked assuming that surely someone, somewhere must know what "public" actually means.[10]

This justification for surveillance and data practices is so common it has become a trope. For example, in 2016 a group of Danish researchers released a data set on nearly seventy thousand users of the popular dating website OkCupid.[11] The researchers used an automated tool called a "scraper" that captures parts of a webpage—a possible violation of the website's terms of use.[12] These users had answered questions on intimate topics like drug use and sexual preferences.[13] The researchers took no steps to de-identify the data set when they released it, despite it being possible to reidentify many of the profiles.[14] When people called out the researchers on Twitter about this lapse, one of them shrugged it off with the flip statement "[d]ata is already public."[15]

[8] More accurately, the SEC prohibits buying or selling securities on the basis of material "nonpublic" information where there is a duty to disclose or refrain from trading. But this concept's inverse implication is that trading on public information is otherwise permissible. *See* 17 C.F.R. § 240.10b5-1 (2018) (outlining duties of individuals who have received insider information and defining insider trading); Selective Disclosure and Insider Trading, Securities Act Release No. 33,7881, Exchange Act Release No. 34,43154, Investment Company Act Release No. IC24599, 65 Fed. Reg. 51,716 (Aug. 24, 2000) (defining "nonpublic" to include information transmitted with expectation of confidentiality).

[9] Federal Policy for the Protection of Human Subjects, 80 Fed. Reg. 53,933, 53,944-45 (proposed Sept. 8, 2015) (proposing allowing researchers to use biospecimens collected from previous studies for future studies without seeking consent when "research is designed not to generate any new information about the person, but only confirm something about them that is already known").

[10] Spoiler alert: no one does.

[11] Brian Resnick, *Researchers Just Released Profile Data on 70,000 OkCupid Users Without Permission*, VOX (May 12, 2016, 6:00 PM), http://www.vox.com/2016/5/12/11666116/70000-okcupid-users-data-release [https://perma.cc/2KG2-SQE5].

[12] Joseph Cox, *70,000 OkCupid Users Just Had Their Data Published*, VICE MOTHERBOARD (May 12, 2016, 1:44 PM), https://motherboard.vice.com/en_us/article/70000-okcupid-users-just-had-their-data-published [https://perma.cc/H63N-AK3W] ("The data was collected between November 2014 to March 2015 using a scraper—an automated tool that saves certain parts of a webpage—from random profiles that had answered a high number of OkCupid's multiple-choice questions.").

[13] *Id.*

[14] Resnick, *supra* note 11 ("The data dump breaks the cardinal rule of social science research ethics: It took identifiable personal data without permission.").

[15] When pushed on the possible privacy problems from this practice, one of the researchers said, "If you don't want other people to see things, don't post them *publicly* on the Internet"

This idea that the "public" nature of information and people justifies information collection, use, and dissemination is rooted in our collective consciousness. Whenever someone's social media posts go viral, people often take great zeal in shooting down any privacy concerns with statements like "Twitter is public."[16] Photographers create advice blog posts with sentiments like "[i]n the United States, public space photography of pretty much anything is legal."[17] Lawyers create advice blog posts that lead off with statements like "[y]ou have no expectation of privacy in anything you do or say in public."[18] It is even encoded in the design of our technologies; social media platforms like Facebook categorize as public information that is not protected by some sort of authentication protocol.[19] This belief is used to justify all kinds of research practices and information flows.[20] The idea is so entrenched that the phrase "there is no privacy in public" has become an almost reflexive defense of certain surveillance and information practices.[21]

Sometimes this argument is justified. What is "public" is often obvious. The halftime performance at the Super Bowl is easy to classify as public under most definitions. But there is trouble at the margins. While privacy scholars for years argued that people should be able to expect a reasonable amount of privacy in public,[22] few inroads have been made. This is partly because the argument gives

and "*Public is public*." Emil O W Kirkegaard (@KirkegaardEmil), TWITTER (May 13, 2016, 12:24 AM) (emphasis added), https://twitter.com/KirkegaardEmil/status/731022196588548096 [https://perma.cc/7RYA-NS35]; Emil O W Kirkegaard (@KirkegaardEmil), TWITTER (May 13, 2016 12:25 AM) (emphasis added), https://twitter.com/KirkegaardEmil/status/731022422930030592 [https://perma.cc/VE25-NLAQ].

[16] Hamilton Nolan, *Twitter Is Public*, GAWKER (March 13, 2014, 12:30 PM), http://gawker.com/twitter-is-public-1543016594 [https://perma.cc/5AAG-KN7H] (arguing public has right to read public tweets).

[17] Jill Corral, *Don't Take My Picture: Street Photography and Public Privacy*, PETAPIXEL (July 29, 2016), https://petapixel.com/2016/07/29/dont-take-picture-street-photography-public-privacy/ [https://perma.cc/Y5PX-E7JH].

[18] Ruth Carter, *No Expectation of Privacy in Public*, CARTER LAW FIRM (June 6, 2013), https://carterlawaz.com/no-expectation-of-privacy-in-public/ [https://perma.cc/AZQ4-96M8].

[19] Michael Zimmer, *''But the Data Is Already Public'': On the Ethics of Research in Facebook*, 12 ETHICS & INFO. TECH. 313, 318-19 (2010) (analyzing researcher's use of "only those data that were accessible by default" to research assistant doing gathering).

[20] *See id.*

[21] *See, e.g.*, *Expect No Privacy in Public Spaces*, THE GLEANER (May 12, 2013, 12:00 AM), http://jamaica-gleaner.com/gleaner/20130512/lead/lead6.html [https://perma.cc/3VL9-4WYZ] ("Once you are in a public space, you have no privacy . . . .").

[22] *See, e.g.*, CHRISTOPHER SLOBOGIN, PRIVACY AT RISK: THE NEW GOVERNMENT SURVEILLANCE AND THE FOURTH AMENDMENT 81 (2007) ("Continuous, repeated, or recorded government surveillance of 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."); DANIEL J. SOLOVE,

the concept of "public information" far too much deference. This deference is understandable—the concept of "public information" is powerful and compelling. But it has come to play a deterministic, linchpin-like role in both law and society that can excuse a host of dubious information practices. This deference to public information is made worse by the fact that the concept in practice is usually best described as "just a hunch."[23]

In this Article, I argue that the "no privacy in public" justification is misguided because nobody knows what "public" means, because it has no set definition in law or policy. Appeals to the public nature of information to justify surveillance and data practices are often just guesswork. At worst, appeals to the public nature of information and acts provide cover for unscrupulous and dangerous data practices and surveillance by making it seem as though there is some objective and established criteria for what constitutes public information. There is no such consensus.[24] The related concept of privacy has been rightfully criticized as too vague or protean.[25] What is meant by terms like "privacy" must

NOTHING TO HIDE: THE FALSE TRADEOFF BETWEEN PRIVACY AND SECURITY 178-81 (2011) (discussing dangers of surveillance and need for increased oversight of government data collection practices); DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 97-100 (2004) [hereinafter SOLOVE, THE DIGITAL PERSON] ("Privacy must be protected by reforming the architecture, which involves restructing our relationships with businesses and the government. In other words, the law should *regulate the relationships* . . . . [I]t involves creating structures to prevent harms from arising rather than merely providing remedies when harms occur."); Patricia Sánchez Abril, *Recasting Privacy Torts in a Spaceless World*, 21 HARV. J.L. & TECH. 1, 6 (2007) (determining that arguments against broader privacy right are "pessimistic, extreme, and deterimental to the development of future technologies and applicable law" and divorces privacy right from space); Jonathan B. Mintz, *The Remains of Privacy's Disclosure Tort: An Exploration of the Private Domain*, 55 MD. L. REV. 425, 440-41 (1996) (rejecting "waiver" justification for public statements); Helen Nissenbaum, *Toward an Approach to Privacy in Public: Challenges of Information Technology*, 7 ETHICS & BEHAV. 207, 208 (1997) (arguing for broader privacy protections in light of mass gathering of personal information); Joel R. Reidenberg, *Privacy in Public*, 69 U. MIAMI L. REV. 141, 157-59 (2014) (arguing for broader protections for speech in public depending on public importance of speech); Zimmer, *supra* note 19, at 323 ("[F]uture researchers must gain a better understanding of the contextual nature of privacy in these spheres, recognizing that just because personal information is made available in some fashion on a social network, does not mean it is fair game for capture and release to all." (citations omitted)).

[23] Or, in the words of the great Inigo Montoya, "You keep using that word. I do not think it means what you think it means." THE PRINCESS BRIDE (Act III Communications 1987).

[24] *See supra* note 22 (detailing disagreement).

[25] *See, e.g.*, DANIEL J. SOLOVE, UNDERSTANDING PRIVACY 1 (2008) ("Privacy . . . is a concept in disarray. Nobody can articulate what it means."); Daniel J. Solove, *Fourth Amendment Pragmatism*, 51 B.C. L. REV. 1511, 1512-13 (2010) ("For a long time, I believed that with the appropriate understanding of privacy—one that is well-adapted to modern technology, nimble and nuanced, forward-looking and sophisticated—Fourth Amendment

be clarified to be useful in law or policy. But in the United States, the concept of public information has been given a free pass.

The goal of this Article is to put to rest the misguided notion of an objective, value-neutral criterion of "public" information for justifying surveillance and data practices. There are several different ways to conceptualize the concept of "public," and they are all value-laden and ideological. This Article highlights the under-theorized and often tautological meanings of "public" and makes the case for clarifying the concept in privacy law to embrace its normative nature.

The concept of "public information" seems intuitive. If it is "out there," it is public—right? But digging deeper, it becomes clear that "public" could mean anything from fleeting exposure to collectively shared knowledge and more. Is the criterion for determining publicness whether it was hypothetically accessible to anyone?[26] Or is "public" anything that is controlled, designated, or released by state actors?[27] Or maybe what is "public" is simply everything that is "not private"?[28]

The main thesis of this Article is that because there are so many different possible interpretations of "public information," the concept cannot be used to justify data practices and surveillance without first articulating a more precise meaning that recognizes what is at stake. By disposing of the myth that there is an objective and dispassionate concept of "public information," judges and lawmakers can clear the way for information rules based on overt value choices. In short, if the concept of "public" is going to shape people's social and legal obligations, its meaning and neutrality should not be assumed.

My argument is based on a fundamental ambiguity in the law of public information: courts and lawmakers have failed to clarify whether the concept is a description, a designation, or just another way of saying that something is "not private." For example, is something "public" because lawmakers and society deem it so, or does something's inherent nature or a certain degree of exposure automatically render it public?[29] Or is it just shorthand for the flipside of the social and legal notions of privacy? This ambiguity has resulted in a confused body of doctrine and frustrated attempts at clear, cogent policy surrounding the

jurisprudence could be rehabilitated. I now realize I was wrong. The entire debate over reasonable expectations of privacy is futile, for it is not focused on the right question.").

[26] *See, e.g.*, Sandler v. Calcagni, 565 F. Supp. 2d 184, 197 (D. Me. 2008) (finding hypothetical accessibility of plaintiff's Myspace page meant information on page was public).

[27] *See infra* Section I.A.3 (discussing public records doctrine and privacy right to those documents).

[28] *See, e.g.*, Donald R.C. Pongrace, *Stereotypification of the Fourth Amendment's Public/Private Distinction: An Opportunity for Clarity*, 34 AM. U. L. REV. 1191, 1196 (1985) (describing "spheres" view where "private" is that which government cannot regulate and "public" is that which it can).

[29] *See* Harry Kalven, Jr., *Privacy in Tort Law—Were Warren and Brandeis Wrong?*, 31 LAW & CONTEMP. PROBS. 326, 327 (1966) (arguing that privacy is that which is left over after government regulations).

collection, use, and disclosure of information. The time has come to end this confusion.

My argument proceeds in three parts. First, I review the law and social discourse of public information. Part I describes the breadth, power, and inconsistency of how policymakers and society talk about public information. The concept is central to many regulatory regimes, yet it is often deployed with little clarification. For example, public information is a key concept in tort law, Fourth Amendment jurisprudence, the law of public records, surveillance statutes, testimonial privileges, intellectual property, and even prohibitions on insider trading.[30] Even when the concept of "public" is given definition, those definitions are both internally inconsistent and inconsistent across bodies of law and jurisdictions. Part I also reviews the way people in society talk and think about public information. How we talk about public acts and information matters because our discourse reflects and shapes our norms and values, which shape law, policy, industry practice, and technological design.[31] Prominent figures such as journalists, activists, critics, and academics sometimes seem to assume the clarity of the concept of "public information" when discussing controversial surveillance and data practices.[32] In this Part, I will show how some invoke this concept regularly to justify surveillance and data practices even when it is not clear what they mean.

Second, I survey the law and literature to propose three different ways to conceptualize "public information." These three notions all work differently in privacy law and policy, serve different values, and cause different problems. Most of the possible meanings are purely *descriptive* in nature. This conceptualization refers to the degree of accessibility, or exposure of acts or data, or the extent to which people have actually seen, processed, or are interested in information. When people equate public information with concepts like "easily accessible," "widely known," and "of interest to society," they are describing a feature, context, or characteristic of acts or data. This conceptualization is often too vague or it fails to match most people's risk assessments about what is or should be "fair game" for data practices and surveillance.

Sometimes public information is defined in *negative* terms—anything that is "not private."[33] Used this way, the notion of publicness is just a synonym for all the things that are not seen as legally or normatively protected acts or practices. That is fair enough. But under this conceptualization, the public nature of

[30] *See supra* notes 4-8 and accompanying text (discussing various applications of privacy across these categories of laws).

[31] Woodrow Hartzog, *The Fight to Frame Privacy*, 111 MICH. L. REV. 1021, 1021 (2013) ("Framing theory holds that even small changes in the presentation of an issue or event can produce significant changes of opinion.").

[32] *See infra* Section II.B (discussing theory that public information is that which is not private information).

[33] *See infra* Section II.B (discussing "not private" theorization of public information).

information cannot be used to avoid privacy protections because it is circular. A judge cannot say "this information is not private because it is public" when what she means is "this information is not private because it is not private." While this conceptualization might be the most common, it is the least helpful as an operative concept in privacy law and policy in defining the scope of people's rights and obligations.

Finally, perhaps the most concrete conceptualization of "public information" applies to things that have been *designated* as such by a relevant authority, such as the State.[34] Public-records laws and other laws, open-data projects, and judicial opinions that explicitly tag acts and practices as fair game for a broad audience all have the advantage of a filtering process with value judgments and risk assessments that facilitate relatively safe and sustainable data practices and surveillance.

In Part III, I make the case for clarity. First, I argue that law and society should treat the notion of "public information" as a value-laden construct that is not self-defining. Thus, whenever the concept of "public information" is invoked to justify surveillance and data practices, it should be scrutinized and clarified. Courts and lawmakers should recognize that, given the indeterminacy and assumptions built into what constitutes public information, the choice of which questions to ask will determine what constitutes what is "public."

I conclude with a proposal to better calibrate notions of public information. Regardless of whether policymakers and society think of "public" as a description, designation, or the inverse of privacy, our analytical frameworks for making that determination are out of whack. There must be some workable way to determine what information should be broadly available to all in the data commons and what sorts of practices are generally acceptable. If everything is private, then nothing is, and we all suffer. To that end, I propose that two concepts should be incorporated into the calculus that determines whether information is public: obscurity and trust. These two concepts play a key role in shaping people's decisions about when, where, how, and with whom to share information or interact with others.

Labeling information or contexts as "public" has important consequences, so we should be intentional and careful about what we choose to label as "public." The publicness of data or acts is too often waived like a talisman to justify a host of information practices like mass surveillance, big-data analytics, and shaming. It is too rarely scrutinized. Often, the surveillance and disclosure practices at issue are desirable. For example, quality journalism and research for the public good are invaluable to society. But other types of surveillance and data practices can be quite harmful.[35] This places privacy policy in a confused and untenable

[34] *See infra* Section II.C (discussing public information as information designated as public).

[35] *See* Julie E. Cohen, *The Biopolitical Public Domain: The Legal Construction of the Surveillance Economy*, 31 PHIL. & TECH. 213, 230-31 (2017) ("The idea of a public domain of personal information sets in motion a familiar and powerful legal and economic just-so

state. How can public information be given such incredible exculpatory power when it has yet to be adequately defined? Designating information as "public" is not a clinical, empirical judgment, but a political, instrumental move. Law and policy should treat it as such. And if the law is going to give the category of "public information" the power to excuse surveillance and data-collection practices, it should be based on something more than "just a hunch."

I. PUBLIC INFORMATION IS A POWERFUL AND ENTRENCHED CONCEPT

Much like Justice Stewart's famous quip about pornography, our laws and discourse about public information seem to be based upon a notion that "[we] know it when [we] see it."[36] Maybe that is why the concept is so prominent when we talk about and regulate privacy. We know the story: if it is public, it is "out there," and is therefore free for others to observe, collect, use, and share. If, on the other hand, it is not public, maybe it is private and there are some rules people need to follow. In this Part, I will review the prominent role, and often significant exculpatory power, bestowed upon the concept of "public information."

A. *The Law of Public Information*

The concept of "public" information is pervasive in the law and often plays a linchpin-like role that determines whether certain restrictions on information or activities will apply. Even though public information is often legally significant, it is usually vaguely defined or not defined at all. This Article focuses on prescriptive conceptualizations of public information that eschew or invite regulatory control precisely because of its public nature.

With respect to the law of privacy, public information has been largely considered fair game from the beginning. Professor Samantha Barbas noted that "judges [at the dawn of the twentieth century] spoke of the absurdity of a right to 'privacy in public.'"[37] A letter to the editor of the *New York Times* in 1902 that was critical of the right to privacy "in public" stated that "[y]ou might just as well prevent a man from taking and using the picture of another man's house or of his horse, . . . unless upon consent."[38] These same sorts of concerns about exercising control over that which was exposed and shared with others have

story. It naturalizes practices of appropriation by data processors and data brokers, positions the new data refineries and their outputs as sites of legal privilege, and elides the connections between information and power. That process subtly and durably reconfigures the legal and economic playing field, making effective regulation of its constituent activities more difficult to imagine.").

[36] Jacobellis v. Ohio, 378 U.S. 184, 197 (1964) (Stewart, J., concurring) ("I shall not today attempt further to define the kinds of material I understand to be embraced within that shorthand description; and perhaps I could never succeed in intelligibly doing so. But I know it when I see it, and the motion picture involved in this case is not that.").

[37] Samantha Barbas, *Saving Privacy from History*, 61 DEPAUL L. REV. 973, 991 (2012).

[38] JNO J. Flynn, Letter to the Editor, *The Right of Privacy*, N.Y. TIMES, July 13, 1902, at 8, https://timesmachine.nytimes.com/timesmachine/1902/07/13/issue.html.

driven the notion of "public information" in privacy law ever since.[39] In this Part, I will review the role that public information and acts play in modern privacy law, including torts, the Fourth Amendment, surveillance statutes, and public records law. I will also review a few other areas of the law that address public information to demonstrate that there is no settled definition for the concept anywhere in the law—but that has not stopped courts and lawmakers from making it a central concept in legal regimes.

1. Torts and "Public Information"

The public disclosure of private facts and intrusion-upon-seclusion torts regularly invoke the concept of "public information" to limit their reach. The *Restatement (Second) of Torts* provides that "[t]here is no liability when the defendant merely gives further publicity to information about the plaintiff that is already public."[40] The *Restatement* authors seem to tether the idea of publicness to theoretical accessibility.[41] Even if facts are "private by nature," there is no liability for publicizing facts that are in some way public or already appear in "public zones."[42] Jonathan Mintz observed that "any facts found in public records, on public streets, in public places of business, inside a public hotel, at school sporting events, or facts that either are public knowledge or have already been publicized, are not actionably private, regardless of their nature."[43]

The rule that there is no privacy in public under the disclosure tort is often described as involving some sort of waiver, consent, or implication that privacy is not to be expected in certain scenarios involving other people.[44] Mintz

[39] *See* Herbert Spencer Hadley, *The Right to Privacy*, 3 NW. L. REV. 1, 11-12 (1894) ("When an individual . . . walks along the streets in the sight of all . . . , he has waived his right to the privacy of his personality."); Mintz, *supra* note 22, at 440-41 (analyzing case law and finding that courts typically find no violation of rights to privacy when information is "public").

[40] RESTATEMENT (SECOND) OF TORTS § 652D cmt. b (AM. LAW INST. 1977).

[41] *See id.* ("On the other hand, if the record is one not open to public inspection . . . , it is not public, and there is an invasion of privacy when it is made so.").

[42] Mintz, *supra* note 22, at 440 ("Publicizing facts that already appear in some zone of the public does not give rise to liability under the disclosure tort, even if the facts are 'private by nature.'" (citing RESTATEMENT (SECOND) OF TORTS § 652D cmt. b (AM. LAW INST. 1977))).

[43] *Id.* (citing Cox Broadcasting Corp. v. Cohn, 420 U.S. 469, 472-73 (1975) then citing Fla. Star v. B.J.F., 491 U.S. 524, 533-36 (1989); then citing Forster v. Manchester, 189 A.2d 147, 150 (Pa. 1963); then citing Gill v. Hearst Publ'g Co., 253 P.2d 441, 444 (Cal. 1953); then citing Jacova v. S. Radio & Television Co., 83 So. 2d 34, 37 (Fla. 1955); then citing McNamara v. Freedom Newspapers, Inc., 802 S.W.2d 901, 905 (Tex. Ct. App. 1991); then citing, in constrast, Daily Times Democrat v. Graham, 162 So. 2d 474, 478 (Ala. 1964); then citing Trout v. Umatilla Cty. Sch. Dist., 712 P.2d 814, 818 (Or. Ct. App. 1985); then citing Heath v. Playboy Enters., Inc., 732 F. Supp. 1145, 1149 (S.D. Fla. 199); then citing W. PAGE KEETON ET AL., PROSSER AND KEETON ON THE LAW OF TORTS § 117, at 856-57 (5th ed. 1984)).

[44] *Id.* at 440-41 (citing *Gill*, 253 P.2d at 444; then citing Dora v. Frontline Video, Inc., 18 Cal. Rptr. 2d 790, 793 (Ct. App. 1993)).

critiqued this rationale as flawed, writing that privacy interests of course recede as the public gains access to the information. Mintz stated, "[I]t is clearly wrong to say that those privacy interests therefore cease to exist and are not worthy of protection. The 'fading' of a privacy interest attendant to a fact's prior public appearance should, instead, raise only a question of degree."[45] He further noted that the most confusing aspect of the "nature and location" element of the disclosure tort is its overlap with the tort's requirement that the matter not be of "legitimate concern to the public."[46]

The concept of "public" gets mangled so often because it is so indeterminate, yet used for several different purposes within elements or factors for a prima facie torts claim. For example, in *Green v. Chicago Tribune Co.*[47] the Illinois Court of Appeals considered whether the Defendant should be liable under the disclosure tort for publishing the Plaintiff's statements and photographs of her son taken surreptitiously in her son's private hospital room.[48] The court relied on the definition of "public place" as articulated in *Black's Law Dictionary*:

> A place to which the general public has a right to resort; not necessarily a place devoted solely to the uses of the public, but a place which is in point of fact public rather than private, a place visited by many persons and usually accessible to the neighboring public (e.g. a park or public beach). Also, a place in which the public has an interest as affecting the safety, health, morals, and welfare of the community. A place exposed to the public, and where the public gather together or pass to and fro.[49]

This definition of a "public place" has two different parts. The idea of a "public place" can be descriptive of *exposure and traffic* (a place visited by many and generally accessible). A place's *effect* on the community as a whole (whatever that means) can determine the definition of a "public place." Ultimately, the court held that the hospital room was not a public place because the "general public" had neither the right to access it nor an interest in that particular hospital room "that affected their safety, health, morals, or welfare."[50] The court did not explicitly define who constituted the "general public" as applied to its interpretation of "public place." It would seem to mean that only certain people would be given permission for entry. Moreover, in *Green*, the court addressed whether the information publicized was a matter of "legitimate public concern."[51] It concluded that, "A jury could find that a reasonable member of the public has no concern with the statements a grieving mother makes to her dead son, or with what he looked like lying dead in the hospital,

[45] *Id.*

[46] *Id.*

[47] 675 N.E.2d 249 (Ill. App. Ct. 1996).

[48] *Id.* at 251.

[49] *Id.* at 252 (quoting *Public Place*, BLACK'S LAW DICTIONARY 1107 (5th ed.1979)).

[50] *Id.*

[51] *Id.* at 255.

even though he died as the result of a gang shooting."[52] To recap, to have an actionable claim under the disclosure tort, one must *share with the public* a matter that is *not already public* and that is not something about which the public should *legitimately concerned*.[53] I used the word "public" three times in that sentence and I am referring to something different each time.

This rule is not absolute. There are some notable exceptions to the general rule that there is no privacy in public information and spaces.[54] However, these have been too few and inconsistent to represent a meaningful resistance to the general assumption that public information is fair game.

2. The Fourth Amendment, Due Process, and "No Reasonable Expectation of Privacy in Public"

Another area where the concept of public information and spaces looms large is the Fourth Amendment. The concept of a "reasonable expectation of privacy" is a central concept that determines the scope of protections under the Fourth Amendment.[55] Some of the confusion around public information and spaces can be traced to the landmark case *Katz v. United States*.[56] Here, Justice Stewart wrote that "[w]hat a person knowingly exposes to the public, even in his own

[52] *Id.* at 256.

[53] *See* 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."); 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, and the gravamen of the tort is publicity as opposed to mere publication. 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)).

[54] *See, e.g.*, Galella v. Onassis, 353 F. Supp. 196, 228 (S.D.N.Y. 1972) (finding "surveillance, close-shadowing and monitoring were clearly 'overzealous' and therefore actionable" when defendant engaged in "corruption of doormen, romancing of the personal maid, deceptive intrusions into children's schools, and return visits to restaurants and stores to inquire about purchases"), *aff'd in part, rev'd in part*, 487 F.2d 986 (2d Cir. 1973); Daily Times Democrat v. Graham, 162 So. 2d 474, 477 (Ala. 1964) (holding that the photograph of woman whose skirt was briefly exposed in public had "nothing of legitimate news value . . . [and] disclose[d] nothing as to which the public is entitled to be informed"); Nader v. Gen. Motors Corp., 255 N.E.2d 765, 771 (N.Y. 1970) ("A person does not automatically make public everything he does merely by being in a public place, and the mere fact that [Plaintiff] was in a bank did not give anyone the right to try to discover the amount of money he was withdrawing. On the other hand, if the plaintiff acted in such a way as to reveal that fact to any casual observer, then, it may not be said that the appellant intruded into his private sphere.").

[55] *See, e.g.*, Katz v. United States, 389 U.S. 347, 351 (1967); Solove, *supra* note 25, at 1512-13.

[56] 389 U.S. 347, 351 (1967).

home or office, is not a subject of Fourth Amendment protection."[57] But then Justice Stewart muddied the conceptual waters by stating in the next sentence "[b]ut what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[58] This opinion hinted at a more nuanced approach to protecting privacy in information and acts that are exposed to others.

But it has not really worked out like that. The equivocal statements in *Katz* led to doctrinal confusion because they are contradictory and conflate several different concepts. How does one avoid knowingly exposing oneself to the public while simultaneously being in an area that is accessible to the public? Judges have been remarkably faithful to the first part of the *Katz* principle of "no privacy in public," notwithstanding the fact that the concept of "publicness" has little more to guide it than a gut instinct or a binary distinction between what is public or private.[59] Usually courts just treat "freely accessible" and "public" as synonyms. Commenting on the trend exacerbated by *Katz*, Professor Brian Serr wrote that instead of refining the reasonable expectation of privacy test, the Supreme Court has focused on what people have "knowingly exposed to the public."[60] In Serr's opinion, "[T]he 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."[61]

---

[57] *Id.* (citing Lewis v. United States, 385 U.S. 206, 210 (1966); then citing United States v. Lee, 274 U.S. 559, 563 (1927)).

[58] *Id.* at 351-52.

[59] *See, e.g.*, Florida v. Jardines, 133 S. Ct. 1409, 1415-16 (2013) (finding right to privacy violated where police conducted canine sniff on Defendant's property); Minnesota v. Carter, 525 U.S. 83, 104 (1998) (Breyer, J., concurring) (arguing that police officer did not violate defendant's Fourth Amendment right when looking into defendant's home from sidewalk); Florida v. Riley, 488 U.S. 445, 450 (1989) (finding no privacy right violation when police saw marijuana on defendant's property in greenhouse from helicopter); California v. Greenwood, 486 U.S. 35, 42 (1988) ("[O]f those state appellate courts that have considered the issue, the vast majority have held that the police may conduct warrantless searches and seizures of garbage discarded in public areas."); California v. Ciraolo, 476 U.S. 207, 211-12 (1986) (holding that ten-foot fence did not give reasonable expectation of privacy to backyard when planes flew over); United States v. Karo, 468 U.S. 705, 711 (1984) (holding that no privacy right was violated when undercover agent placed tracking device in can of ether later sold to defendant); United States v. Knotts, 460 U.S. 276, 281-82 (1983) ("A person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another. When [Defendant] traveled over the public streets he voluntarily conveyed to anyone who wanted to look the fact that he was traveling 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.").

[60] Brian J. Serr, *Great Expectations of Privacy: A New Model for Fourth Amendment Protection*, 73 MINN. L. REV. 583, 597-98 (1988-1989) (footnotes omitted).

[61] *Id.* at 598.

This trend to distill people's reasonable expectations of privacy down to a binary world with purportedly clear lines is evident in both federal and state case law. For example, the Washington Supreme Court held:

> Police may surreptitiously follow a suspect to collect DNA, fingerprints, footprints, or other possibly incriminating evidence, without violating that suspect's privacy. No case has been cited challenging or declaring this type of police practice unreasonable or unconstitutional. People constantly leave genetic material, fingerprints, footprints, or other evidence of their identity in public places. There is no subjective expectation of privacy in discarded genetic material just as there is no subjective expectation of privacy in fingerprints or footprints left in a *public place*. Physical characteristics which are *exposed to the public* are not subject to Fourth Amendment protection.[62]

In arguing against the majority's holding regarding whether using a thermal imaging device violated the Fourth Amendment, Justice Stevens stated in his dissent in *Kyllo v. United States*[63] that "[h]eat waves, like aromas that are generated in a kitchen, or in a laboratory or opium den, enter the public domain if and when they leave a building."[64] Justice Stevens argued that "emissions in the public domain" include "excessive heat, traces of smoke, suspicious odors, odorless gases, airborne particulates, or radioactive emissions" and "the process of drawing inferences from data in the public domain should not be characterized as a search."[65]

---

[62] State v. Athan, 158 P.3d 27, 37 (Wash. 2007) (emphasis added). Other courts have held that checking a vehicle identification number ("VIN") in a public place is not a search. *See, e.g.*, State v. Halczyszak, 496 N.E.2d 925, 933 (Ohio 1986) ("[T]he mere act of viewing a VIN is not a search within the meaning of the Fourth Amendment so long as police are lawfully in a position to make the observation. Nor can it be rationally concluded that a computer check of the VIN is more violative of the Fourth Amendment than viewing it. Consequently we hold that police may make computer checks of lawfully obtained VINs where their purpose is to negate or establish whether the auto is stolen."); State v. Anderson, No. 24678, 2012 WL 376691, at *2 (Ohio Ct. App. Feb. 3, 2012) ("We disagree with the trial court's conclusion that Anderson had a reasonable expectation of privacy in the spaces immediately adjacent to the vehicles—i.e., his leased space—as against persons who were on the lot with permission of the owner."). *But see* United States v. Jones, 565 U.S. 400, 430 (2012) (Alito, J., concurring) ("But the use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy. For such offenses, 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."); Kyllo v. United States, 533 U.S. 27, 34 (2001) (finding that "[t]o withdraw protection of this minimum expectation [of privacy] would be to permit police technology to erode the privacy guaranteed by the Fourth Amendment" but still relying on public/private dichotomy and looking to "public use" to determine scope of privacy).

[63] 533 U.S. 27 (2001).

[64] *Id.* at 43-44 (Stevens, J., dissenting).

[65] *Id.* at 45, 49.

There is some movement in the past few years to add nuance to the public information and spaces concept in the Fourth Amendment.[66] However, so long as courts continue to implicitly validate the idea of public information and spaces as a settled, objective construct, meaningful change will be difficult. "Public" information remains a broadly defined showstopper.

3. Public Records

The importance of the concept of "public" is evident in public-records regimes. It is right there in the name. Generally, public-records laws dictate the types of records created or stored by government entities that will be made available to anyone who requests them and the circumstances under which they will be released or withheld.[67] But the concept of public records also has blurry edges. *Black's Law Dictionary* defines a public record as "a register of the legal transactions, proceeding, rules and statutes, laws and regulations that is kept on

[66] *See, e.g.*, *Jones*, 565 U.S. at 417-18 (Sotomayor, J., concurring) ("[I]t may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties . . . . I 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.").

[67] *See, e.g.*, CAL. GOV'T CODE § 6252 (West 2016) (defining "Public records" to include "any writing containing information relating to the conduct of the public's business prepared, owned, used, or retained by any state or local agency regardless of physical form or characteristics. 'Public records' in the custody of, or maintained by, the Governor's office means any writing prepared on or after January 6, 1975"); *id.* § 15652 (mandating procedures and guidelines to "facilitate maximum public accessibility to the [State Board of Equalization's] public records"); MASS. GEN. LAWS ch. 66, § 10 (2017) ("Every person having custody of any public record, as defined in clause Twenty-sixth of section seven of chapter four, shall, at reasonable times and without unreasonable delay, permit it, or any segregable portion of a record which is an independent public record, to be inspected and examined by any person, under his supervision, and shall furnish one copy thereof upon payment of a reasonable fee."); 38 R.I. GEN. LAWS § 38-2-2 (2018) (describing public record emails as those "made or received pursuant to law or ordinance or in connection with the transaction of official business by any agency"); Keddie v. Rutgers, State Univ., 689 A.2d 702, 709 (N.J. 1997) ("The common-law definition of a public record is broader than the definition of a Right-to-Know document ["RTKL"]. A common-law record is one that is made by a public official in the exercise of his or her public function, either because the record was required or directed by law to be made or kept, or because it was filed in a public office. Thus, all RTKL documents are common-law records as well. But not all common-law records are RTKL documents. Unlike RTKL documents, the right to access common-law records is a qualified one." (citations omitted)); Bergen Cty. Improvement Auth. v. N. Jersey Media Grp., Inc., 851 A.2d 731, 740 (N.J. Super. Ct. App. Div. 2004) ("Once a court is satisfied that the information requested is a 'public record,' it must then ascertain whether the requestor has a cognizable interest in the subject matter contained in the material. Assuming such an individual interest is found, a court must determine whether the individual's right of access outweighs the State's interest in preventing disclosure.").

file to be able to be referred to if needed."[68] One of the central conflicts in the law of public records is determining which public records should be ultimately released based on certain policy considerations, including privacy.[69]

Tagging and releasing information as a public record has two important functions. First, it makes information more accessible and thus more likely to be seen. Second, the designation of information as a "public record" can affect how lawmakers, judges, industry, media, and society view people's privacy interest in the relevant information.[70] In other words, public-records regimes can have a bootstrapping effect on personal information. The relative privacy in personal information that is released as a public record is first diminished when the government discloses it. Then the fact that the information was made "public" is used to defeat any future claims for a privacy violation.[71] The public nature of such records exists in name and in practice.

Public-records issues get particularly thorny when they are aggregated into massive data sets that dramatically reduce the search costs for the curious or

[68] *Public Record*, BLACK'S LAW DICTIONARY (online 2d ed.), https://thelawdictionary.org/public-record/ [https://perma.cc/3G8P-LW46] (last visited Feb. 15, 2019).

[69] *See* David S. Ardia & Anne Klinefelter, *Privacy and Court Records: An Empirical Study*, 30 BERKELEY TECH. L.J. 1807, 1826 (2015); Grayson Barber, *Personal Information in Government Records: Protecting the Public Interest in Privacy*, 25 ST. LOUIS U. PUB. L. REV. 63, 63 (2006); Amanda Conley et al., *Sustaining Privacy and Open Justice in the Transition to Online Court Records: A Multidisciplinary Inquiry*, 71 MD. L. REV. 772, 839-45 (2012); Jane E. Kirtley, *"Misguided in Principle and Unworkable in Practice": It Is Time to Discard the Reporters Committee Doctrine of Practical Obscurity (and Its Evil Twin, the Right to Be Forgotten)*, 20 COMM. L. & POL'Y 91, 109 (2015); Samuel A. Terilli & Sigman L. Splichal, *Public Access to Autopsy and Death-Scene Photographs: Relational Privacy, Public Records and Avoidable Collisions*, 10 COMM. L. & POL'Y 313, 319 (2005).

[70] *See* Cox Broad. Corp. v. Cohn, 420 469, 491 (1975); Mintz, *supra* note 22, at 449-50 (discussing *Cox Broadcasting Corp. v. Cohn* whereby the Supreme Court ruled unconstitutional the conviction of a reporter under a Georgia statute making the publication of a rape victim's name a misdemeanor offense). The Court in *Cox* "declared that a State may not 'impose sanctions on the accurate publication of the name of a rape victim obtained from public records—more specifically, from judicial records which are maintained in connection with a public prosecution and which themselves are open to public inspection.'" *Id.* at 449 (quoting *Cox Broad. Corp.*, 420 U.S. at 491). Mintz noted that "[t]he presence of the rape victim's name—'truthful information'—in 'official court records open to public inspection' was the gravamen of the Court's analysis." *Id.* (footnote omitted). Moreover, "[t]he Court noted that such information was 'in the public domain.'" *Id.* "According to the majority, the privacy interest had therefore faded, a conclusion that was especially 'compelling when viewed in terms of the First and Fourteenth Amendments and in light of the public interest in a vigorous press.'" *Id.* at 449-50 (footnote omitted). The Federal Rules of Evidence provide that public records are an exception to the rule against hearsay. *See* FED. R. EVID. 803(8).

[71] *See Cox*, 420 U.S. at 495 ("By placing the information in the public domain on official court records, the State must be presumed to have concluded that the public interest was thereby being served.").

when they include information that is already "public."[72] For example, the government regularly compels people to disclose information like their name; age; address; their photograph and physical description; the identity and names of all their close relatives, parents, siblings, and children; and certain activities and transgressions relevant to court proceedings.[73] Courts and lawmakers regularly consider much of this information public, perhaps because we expose and share this information with others all the time. Does that mean that as public records there is no privacy interest that should affect this information's official release? What about limited types of disclosures, like our protected social media accounts and fleeting exposures that were theoretically out in the open but in reality were only actually seen by a few people?

In *U.S. DOJ v. Reporters Committee for Freedom of the Press*[74] the Supreme Court was asked whether there was a privacy interest in a criminal "rap sheet" containing aggregated public records.[75] The Court found a privacy interest in information that was technically available as a public record but could only be found by spending a burdensome and unrealistic amount of time and effort in obtaining and aggregating it.[76] The information was considered "practically obscure" because of the extremely high cost and low likelihood of the public compiling the information.[77] Specifically, the Court stated that while criminal identification records are "a matter of public record, the availability and dissemination of [this information] to the public is limited."[78] The Court observed that "[t]he very fact that federal funds have been spent to prepare, index, and maintain [the] criminal-history files demonstrates that the individual items of information in the summaries would not otherwise be 'freely available' either to the officials who have access to the underlying files or to the general public."[79]

Accordingly, the Court characterized the issue in the case as "whether the compilation of otherwise hard-to-obtain information alters the privacy interest implicated by disclosure of that information."[80] Ultimately, the Court concluded

[72] *See* Daniel J. Solove, *Access and Aggregation: Public Records, Privacy and the Constitution*, 86 MINN. L. REV. 1137, 1138 (2002) (highlighting aggressive techniques and requests for government acquiring and declaring public vast amounts of personal information); *see also* David S. Ardia & Anne Klinefelter, *supra* note 69, at 1808 (discussing "sensitive information" in increasingly public court records); Amanda Conley et al., *supra* note 69, at 777 ("[C]ourts have an obligation to rewrite rules governing the creation of, and access to, public court records in light of substantive changes that online access augurs.").

[73] *See* Solove, *supra* note 72, at 1182-84.

[74] 489 U.S. 749 (1989).

[75] *Id.* at 751.

[76] *Id.* at 764.

[77] *Id.* at 780.

[78] *Id.* at 753.

[79] *Id.* at 764.

[80] *Id.*

that "there is a vast difference between the public records that might be found after a diligent search of courthouse files, county archives, and local police stations throughout the country and a computerized summary located in a single clearinghouse of information."[81] Hence, the Court held that disclosure of the information contained in the criminal identification records "'could reasonably be expected to constitute an unwarranted invasion of personal privacy' within the meaning of the Freedom of Information Act."[82]

The Court noted that under the common law, "one did not necessarily forfeit a privacy interest in matters made part of the public record, albeit the privacy interest was diminished and another who obtained the facts from the public record might be privileged to publish it."[83] The *Restatement (Second) of Torts* draws the line at accessibility, however, stating that:

> [T]here is no liability for giving publicity to facts about the plaintiff's life that are matters of public record, such as the date of his birth . . . . On the other hand, if the record is one not open to public inspection, as in the case of income tax returns, it is not public, and there is an invasion of privacy when it is made so.[84]

Another body of doctrine looks to the newsworthiness of information to determine its privacy interests, not just whether it is a public record. "[M]erely because [a fact] can be found in a public record, does not mean that it should receive widespread publicity if it does not involve a matter of public concern."[85]

Professor Helen Nissenbaum noted the paradox inherent in public records, observing that people worry about putting public records online, even though they are already theoretically accessible to all.[86] In reality, most personal information is shared with some, but not all.[87] As I will discuss below, this reality does not mesh well with most legal notions of public information.

---

[81] *Id.*

[82] *Id.* at 751, 780 (holding, inter alia, that "a third party's request for law enforcement records or information about a private citizen can reasonably be expected to invade that citizen's privacy").

[83] *Id.* at 763 n.15 (citing Cox Broad. Corp. v. Cohn, 420 U.S. 469, 494-95 (1975)).

[84] RESTATEMENT (SECOND) OF TORTS § 652D (AM. LAW INST. 1977).

[85] KEETON ET AL., *supra* note 43, at 859.

[86] Helen Nissenbaum, *Privacy as Contextual Integrity*, 79 WASH. L. REV. 119, 120-21 (2004).

[87] *Id.*; *see* SOLOVE, THE DIGITAL PERSON, *supra* note 22, at 97-100; Lior Jacob Strahilevitz, *A Social Networks Theory of Privacy*, 72 U. CHI. L. REV. 919, 920-21 (2005) ("Despite the centrality of this issue, the American courts lack a coherent, consistent methodology for determining whether an individual has a reasonable expectation of privacy in a particular fact that has been shared with one or more persons. Indeed, jurisdictions cannot agree on a framework for resolving these kinds of cases.").

The court in *Doe v. City of New York*[88] observed that "[c]ertainly, there is no question that an individual cannot expect to have a constitutionally protected privacy interest in matters of public record,"[89] yet held in this instance that:

> Doe has a right to privacy (or confidentiality) in his HIV status, because his personal medical condition is a matter that he is normally entitled to keep private. We also hold that Doe's HIV status did not, as a matter of law, automatically become a public record when he filed his claim with the Commission and entered into the Conciliation Agreement.[90]

Here it would appear the sensitivity of the information was operative in the ultimate determination of whether information was public.

Professor Daniel Solove observed that public records pose a threat to privacy, stating, "From the beginning of the twentieth century, we have witnessed a vast proliferation in the number of government records kept about individuals as well as a significant increase in public access to these records."[91] According to Solove, "These trends together have created a problematic state of affairs—a system where the government extracts personal information from the populace and places it in the public domain, where it is hoarded by private sector corporations that assemble dossiers on almost every American citizen."[92] Sometimes court records go "back in the vault," and people get upset, demonstrating that not all forms of "public" records are equal.[93]

4. Related Concepts: Nonpublic Information, Public Domains, Publication, Publicity, and "the Public"

The idea of "public information" is also relevant in a number of different statutory and common law regimes unrelated (or only tangentially related) to privacy. Some laws only target "nonpublic" information, which is another way of saying that public information is outside the scope of the statute. Others use concepts of publicness to define the scope of people's rights (such as the right to control "public" performance or a copyrighted work) or to designate a space free from rules, restrictions, and property rights (such as the "public domain"). A review of the role of public information in these diverse bodies of law reveals that even though the notion of "public information" is often relevant and even decisive, it is often poorly conceptualized with no consistent definition.

---

[88] 15 F.3d 264 (2d Cir. 1994).

[89] *Id.* at 268.

[90] *Id.* at 269 (citations omitted).

[91] Solove, *supra* note 72, at 1142.

[92] *Id.*

[93] Joe Mullin, *US Courts Trash a Decade's Worth of Online Documents, Shrug it Off*, ARS TECHNICA (Aug. 26, 2014, 5:45 PM), http://arstechnica.com/tech-policy/2014/08/us-courts-trash-a-decades-worth-of-documents-shrug-it-off/ [https://perma.cc/KZ57-QGUV] ("The Administrative Office of the US Courts (AO) has removed access to nearly a decade's worth of electronic documents from four US appeals courts and one bankruptcy court.").

a. *Insider Trading on Nonpublic Information*

The SEC has passed rules that prohibit, among other things, buying or selling securities on the basis of material nonpublic information in certain circumstances, otherwise known as insider trading.[94] These regulations are designed to ensure fairness in the markets and prevent individuals from exploiting information through an abuse of trust and confidence, rather than through the use of investigation and skill.[95]

Generally, nonpublic information is defined as information that "has not been disseminated in a manner making it available to investors generally."[96] That is an ambiguous definition.[97] Must the information merely be made available to the investing public, or must it be effectively disseminated?[98] Blog posts written

[94] *See* sources cited *supra* note 8. Professor Thomas Lee Hazen explains:

> Trading on inside information can occur in various contexts. First, there is what is often referred to as "classical" insider trading, which consists of those instances in which a true company insider, such as an officer or director, trades on nonpublic information she acquired as a result of her special and fiduciary position with the company. Second, there are cases where an insider passes on this information to someone else—referred to as "tipper/tippee" liability. Finally, as noted above, there are those instances often referred to as "outsider" trading, where someone who does not have a special relationship to the company acquires information about the company and improperly trades on that information; these are most often referred to as the "misappropriation" cases.

Thomas Lee Hazen, *Identifying the Duty Prohibiting Outsider Trading on Material Nonpublic Information*, 61 HASTINGS L.J. 881, 890 (2010) (citations omitted).

[95] Troy Cichos, *The Misappropriation Theory of Insider Trading: Its Past, Present, and Future*, 18 SEATTLE U. L. REV. 389, 424 (1995) (describing "underlying goals" as "fairness and equal opportunity").

[96] SEC v. Tex. Gulf Sulphur Co., 401 F.2d 833, 854 (2d Cir. 1968) ("Before insiders may act upon material information, such information must have been effectively disclosed in a manner sufficient to insure its availibility to the investing public."); Inv'rs Mgmt. Co., Exchange Act Release No. 34,9267, 44 SEC Docket 633 (July 29, 1971).

[97] *See* Donald C. Langevoort, *"Fine Distinctions" in the Contemporary Law of Insider Trading*, 2013 COLUM. BUS. L. REV. 429, 457 (using examples to explain downfalls of ambiguous defintion); Carol B. Swanson, *Insider Trading Madness: Rule 10b5-1 and the Death of Scienter*, 52 U. KAN. L. REV.147, 150 n.14 (2003) ("The insider trading concept has been endlessly criticized as ill-defined."). Even in disputes over the proper classification of information within this rule, some courts have seemingly assumed that information was "nonpublic" with little discussion. *See, e.g.*, SEC v. Happ, 392 F.3d 12, 34 (1st Cir. 2004) (refusing to find that district court abused its discretion in rejecting SEC argument for public information).

[98] *See* Joel Seligman, *The Reformulation of Federal Securities Law Concerning Nonpublic Information*, 73 GEO. L.J. 1083, 1139 (1985) (addressing ongoing questions looming over an unclear definition); *cf.* Barbara Bader Aldave, *Misappropriation: A General Theory of Liability for Trading on Nonpublic Information*, 13 HOFSTRA L. REV. 101, 122 (1984) ("Properly understood, the misappropriation theory [of insider trading] only bars trading on the basis of information that the wrongdoer converted to his own use in violation of some fiduciary, contractual, or similar obligation to the owner or rightful possessor of the information.").

under a pseudonym and not searchable by Google (but technically available to anyone with the right URL) can be described as available. Information in a major newspaper or popular LISTSERV is more effectively disseminated.

In their dissent in *Chiarella v. United States*,[99] Justices Blackmun and Marshall keenly noted the importance between these two requirements, stating:

> [T]here is a significant conceptual distinction between parity of information and parity of *access* to material information. The latter gives free rein to certain kinds of informational advantages that the former might foreclose, such as those that result from differences in diligence or acumen. Indeed, by limiting opportunities for profit from manipulation of confidential connections or resort to stealth, equal access helps to ensure that advantages obtained by honest means reap their full reward.[100]

This tension between mere availability and effective dissemination, which has a dramatic effect on probabilities of exposure and transaction costs, lies at the heart of the problem with public information.

The same kind of tension is often relevant in determining whether certain disclosures were confidential. For example, courts often use concepts of "publicness" when determining whether a spousal privilege, attorney-client privilege, or other right based upon a confidential relationship has been waived.[101]

---

[99] 445 U.S. 222 (1980).

[100] *Id.* at 252 n.2 (Blackmun, J., dissenting); *see* Ronald F. Kidd, Note, *Insider Trading: The Misappropriation Theory Versus an "Access to Information" Perspective*, 18 DEL. J. CORP. L. 101, 133 (1993) ("[T]he Court has never clearly defined what it means by the 'parity/equality of information theory' in either *Chiarella* or *Dirks*. There are two possible interpretations of the theory referred to by the Court; each has a different outcome. The Court may mean that *all* information, public and nonpublic, held by one party must be disclosed to the other party. Alternatively, the majority may have been referring to what this note has termed the 'access to information' theory. The former would discourage legitimate information gathering efforts. It would be pointless to engage in legitimate information gathering efforts, because any pertinent information that was uncovered would have to be disclosed to the other party, thus resulting in complete 'parity and equality' of information. This result is certainly unacceptable. The latter, however, does not have this effect because it only prohibits investors from using information *not legally discoverable* by other parties.").

[101] *See* United States v. Corbin, 729 F. Supp. 2d 607, 610 (S.D.N.Y. 2010) ("[T]he Communications Firm had confidentiality policies in place, and distributed them to its employees. These policies made clear that each employee had a duty to maintain the confidentiality of nonpublic information related to the firm's clients to which they were privy."); *In re* Warner, 2005-303 (La. 4/17/09); 21 So. 3d 218, 232 ("Rule XIX, § 16(A) defines what information should be considered nonpublic or confidential as it regards attorney disciplinary matters . . . ."); People v. Hayes, 35 N.E. 951, 954 (N.Y. 1894) ("[W]hen the husband or wife, to whom a written confidential communication is addressed, makes it public by giving it to another, the confidential character of the communication as against such party has departed and it may be treated like any other communication and put in evidence if otherwise admissible."); 17 C.F.R. § 240.10b5-2(b) (2018) ("[A] 'duty of trust or confidence'

b. *Nonpublic Personally Identifiable Information*

The concept of "public information" is often a prominent part of a key threshold privacy law concept known as "personally identifiable information." Professors Paul Schwartz and Daniel Solove note that "[i]nformation privacy law rests on the currently unstable category of Personally Identifiable Information (PII)" and that "[i]nformation that falls within this category is protected, and information outside of it is not."[102] Unfortunately, there is no set definition for PII, which has created many inconsistencies and problems within legal regimes. Schwartz and Solove note that one way regulatory regimes define PII is anything that is "non-public"[103] writing:

> The non-public approach seeks to define PII by focusing on what it is *not*, rather than on what it is . . . . Instead of saying that PII is simply that which identifies a person, the non-public approach draws on concepts of information that is publicly accessible and information that is purely statistical.[104]

For example, the Gramm-Leach-Bliley Act ("GLBA") makes extensive use of the concept of "nonpublic" information to articulate the kind of information

exists in the following circumstances, among others: (1) Whenever a person agrees to maintain information in confidence; (2) Whenever the person communicating the material nonpublic information and the person to whom it is communicated have a history, pattern, or practice of sharing confidences, such that the recipient of the information knows or reasonably should know that the person communicating the material nonpublic information expects that the recipient will maintain its confidentiality; or (3) Whenever a person receives or obtains material nonpublic information from his or her spouse, parent, child, or sibling; *provided*, however, that the person receiving or obtaining the information may demonstrate that no duty of trust or confidence existed with respect to the information . . . ."); Ore. Evid. Code, Rule 505(1)(a) cmt. ("A communication made in public or meant to be relayed to outsiders can scarcely be considered confidential. Unless intent to disclose is apparent, a communication between husband and wife is confidential."); Annotation, *Effect of Knowledge of Third Person Acquired by Overhearing or Seeing Communication Between Husband and Wife upon Rule as to Privileged Communication*, 63 A.L.R. 107 (1929) ("In Freeman v. Freeman (1921) 238 Mass. 150, 130 N.E. 220, it was held that neither spouse might testify as to a conversation between them *in a public street*, where it did not appear that any of the passers-by or persons in their vicinity paid any attention to them, or even could hear the words. But in Linnell v. Linnell (1924) 249 Mass. 51, 143 N.E. 813, it was held that a husband may testify as to a conversation between himself and his wife which *occurred in the public waiting room* of a railroad station, where it appeared that there was a crowd about them all the time, and that anyone who had been listening could have heard the conversation within 4 or 5 feet from where they were standing,—the circumstances being such that it could not have been ruled as a matter of law that what was said by the parties, in a room where thirty or forty other persons were present, was a private conversation." (emphasis added)).

[102] Paul M. Schwartz & Daniel J. Solove, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, 86 N.Y.U. L. REV. 1814, 1816 (2011).

[103] *Id.* at 1829-30.

[104] *Id.*

that falls within the statute's ambit.[105] The regulations promulgated under the statute exclude from the definition of "nonpublic" information that is "publicly available."[106] The statute defines "publicly available" in a broad, schizophrenic, and sometimes circular way, leading us back to the public information fallacy. The statute defines publicly available information as "any information that you have a reasonable basis to believe is lawfully made available to the general public from" government records, widely distributed media, or legally mandated public disclosures.[107] It goes on to provide that:

> You have a reasonable basis to believe that information is lawfully made available to the general public if you have taken steps to determine: (i) That the information is of the type that is available to the general public; and (ii) Whether an individual can direct that the information not be made available to the general public and, if so, that your consumer has not done so.[108]

[105] Specifically, the regulations implementing the GBLA provide:

> Nonpublic personal information means: (i) Personally identifiable financial information; and (ii) Any list, description, or other grouping of consumers (and *publicly available* information pertaining to them) that is derived using any personally identifiable financial information that is *not publicly available*. (2) *Nonpublic* personal information does not include: (i) Publicly available information, except as included on a list described in paragraph (n)(1)(ii) of this section; or (ii) Any list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived without using any personally identifiable financial information that is not publicly available. (3) Examples of lists—(i) Nonpublic personal information includes any list of individuals' names and street addresses that is derived in whole or in part using personally identifiable financial information (that is not publicly available), such as account numbers. (ii) Nonpublic personal information does not include any list of individuals' names and addresses that contains only publicly available information, is not derived, in whole or in part, using personally identifiable financial information that is not publicly available, and is not disclosed in a manner that indicates that any of the individuals on the list is a consumer of a financial institution.

16 C.F.R. § 313.3(n)(1) (2018) (emphasis added).

[106] *Id.*

[107] *Id.* § 313.3(p)(1).

[108] *Id.* § 313.3(p)(2) ("(3) *Examples*—(i) *Government records.* Publicly available information in government records includes information in government real estate records and security interest filings. (ii) *Widely distributed media*. Publicly available information from widely distributed media includes information from a telephone book, a television or radio program, a newspaper, or a web site that is available to the general public on an unrestricted basis. A web site is not restricted merely because an Internet service provider or a site operator requires a fee or a password, so long as access is available to the general public. (iii) *Reasonable basis*— (A) You have a reasonable basis to believe that mortgage information is lawfully made available to the general public if you have determined that the information is of the type included on the public record in the jurisdiction where the mortgage would be recorded. (B) You have a reasonable basis to believe that an individual's telephone number is lawfully made available to the general public if you have located the telephone number in the telephone book or the consumer has informed you that the telephone number is not unlisted.").

In summary, the GLBA excludes "publicly available information" from the definition of "nonpublic personal information." Information is "publicly available" if, among other things, it was widely distributed in the media. This conceptualization initially sounds like it might conceptualize "availability" in terms of effective dissemination rather than theoretical accessibility. However, in the examples for what constitutes "widely distributed media," it includes a "web site that is available to the general public on an unrestricted basis."[109] This could be anything from CNN.com to my cousin's family blog that uses no names, is not indexed by Google, and is read by a total of about twelve people. As I will discuss below, broad definitions of "public" that are built around a lack of authentication restrictions and theoretical accessibility are profoundly broken.

c. *The Public Domain*

Another significant legal construct that relies heavily on notions of publicness is "the public domain." As a general term, "the public domain" is hard to define, but it plays a prominent role in the law of intellectual property, among other things. Within intellectual property regimes, the public domain has been defined as "the realm embracing property rights that belong to the community at large, are unprotected by copyright or patent, and are subject to appropriation by anyone."[110] The term is commonly thought of as "material that is not covered by intellectual property rights."[111] Though Professor James Boyle notes, "Some definitions of the public domain are more granular. They focus not only on complete works but on the reserved spaces of freedom inside intellectual property."[112] Boyle himself explores how the public domain can be like "the opposite of property."[113]

For example, the Supreme Court in *Harper & Row, Publishers, Inc. v. Nation Enterprises*[114] stated that:

> [C]opyright does not prevent subsequent users from copying from a prior author's work those constituent elements that are not original—for example, quotations borrowed under the rubric of fair use from other copyrighted works, facts, or materials in the public domain—as long as such use does not unfairly appropriate the author's original contributions.[115]

[109] *Id.*

[110] *Public Domain*, MERRIAM-WEBSTER'S COLLEGIATE DICTIONARY (11th ed. 2012).

[111] JAMES BOYLE, THE PUBLIC DOMAIN: ENCLOSING THE COMMONS OF THE MIND 57 (2009).

[112] *Id.*

[113] *Id.* ("The opposite of property, or perhaps we should say the *opposites* of property, are much more obscure to us than property itself.").

[114] 471 U.S. 539 (1985).

[115] *Id.* at 548.

Items in the public domain are "not protected by copyright law and are available for use without permission. Often, works enter the public domain after patent, copyright, or trademark rights have expired or been abandoned."[116]

Despite the centrality of the public domain in our everyday lives as well as within intellectual property regimes, scholars, courts, and policymakers struggle to conceptualize the edges of the public domain and differ on its proper role in property and surveillance regimes.[117] The public domain often embodies what I call the negative conceptualization of public information—defined not by what it is, but by what it is not.[118]

d. *Public Performance and Public Use*

Two other intellectual property constructs that rely upon notions of publicness are the concepts of public performance and public use. Understanding how these concepts operate and their inherent problems can be instructive for understanding public information in privacy law. The public-use doctrine acts as a bar to patent registration and applies when a device "used in public includes every limitation of [a] later claimed invention . . . and the device used would have been obvious to one of ordinary skill in the art."[119] In order to constitute a

[116] *Public Domain*, NOLO'S PLAIN-ENGLISH LAW DICTIONARY, https://www.nolo.com/dictionary/public-domain-term.html [https://perma.cc/5M24-YN9G] (last visited Feb. 15, 2019).

[117] *See, e.g.*, Cohen, *supra* note 35, at 230-31; Jessica Litman, *The Public Domain*, 39 EMORY L.J. 965, 975-77 (1990) ("The concept of the public domain is another import from the realm of real property. In the intellectual property context, the term describes a true commons comprising elements of intellectual property that are ineligible for private ownership." (citations omitted)); Tyler T. Ochoa, *Is the Copyright Public Domain Irrevocable? An Introduction to* Golan v. Holder, 64 VAND. L. REV. EN BANC 123, 124 (2011) ("The public domain may be defined as that body of literary and artistic works (or other information) that is not subject to any copyright (or other intellectual property right), and which therefore may be freely used by any member of the general public."); Tyler T. Ochoa, *Origins and Meanings of the Public Domain*, 28 U. DAYTON L. REV. 215, 217-22 (2003) [hereinafter Ochoa, *Origins and Meanings*] (providing overview of public domain meaning); Pamela Samuelson, *Enriching Discourse on Public Domains*, 55 DUKE L.J. 783, 783-813 (2006); Pamela Samuelson, *Mapping the Digital Public Domain: Threats and Opportunities*, 66 LAW & CONTEMP. PROBS. 147, 149-52 (2003) ("Although I define the public domain as a sphere in which contents are free from intellectual property rights, there is another murky terrain near the boundaries of the public domain consisting of some intellectual creations that courts have treated as in the public domain for some, but not all, purposes.").

[118] Ochoa, *Origins and Meanings*, *supra* note 117, at 221-22.

[119] Netscape Commc'ns Corp. v. Konrad, 295 F.3d 1315, 1321 (Fed. Cir. 2002) (citations omitted); *see also* Bonito Boats, Inc. v. Thunder Craft Boats, Inc., 489 U.S. 141, 150 (1989) ("Taken together, the novelty and nonobviousness requirements express a congressional determination that the purposes behind the Patent Clause are best served by free competition and exploitation of either that which is already available to the public or that which may be readily discerned from publicly available material.").

public use for the purposes of patent law, an invention must be used for its intended purpose.[120]

Yet it is not always clear what the term "public" means in this context. In one of the earliest and most famous public use cases, *Egbert v. Lippmann*,[121] the Supreme Court found that a single embodiment of an invention that could not be seen by "the public eye" (in this case an improvement for a corset spring) when disclosed to a single person (the wearer of the corset-springs who was not the inventor) was enough to bar the patent based upon public use.[122] In essence, one person was the public. The Court elaborated, stating:

> [W]hether the use of an invention is public or private does not necessarily depend upon the number of persons to whom its use is known. If an inventor, having made his device, gives or sells it to another, to be used by the donee or vendee, without limitation or restriction, or injunction of secrecy, and it is so used, such use is public, even though the use and knowledge of the use may be confined to one person.[123]

Copyright owners have the exclusive right to the public performance of their works.[124] Yet the definition of "public performance" is not always clear. The Copyright Act provides:

> To perform or display a work "publicly" means—(1) to perform or display it at a place open to the public or at any place where a substantial number of persons outside of a normal circle of a family and its social acquaintances is gathered; or (2) to transmit or otherwise communicate a performance or display of the work to a place specified by clause (1) or to the public, by means of any device or process, whether the members of the public capable of receiving the performance or display receive it in the same place or in separate places and at the same time or at different times.[125]

In *Columbia Pictures Industries, Inc. v. Redd Horne Inc.*,[126] the Third Circuit Court of Appeals was asked to determine if the playing of a video cassette in a private room that was located inside of a video rental store that was open to the

---

[120] Motionless Keyboard Co. v. Microsoft Corp., 486 F.3d 1376, 1384 (Fed. Cir. 2007) ("[T]he Court determined that the invention had been used for its intended purpose for over a decade without limitation or confidentiality requirements. Thus, even though not in public view, the invention was in public use.").

[121] 104 U.S. 333 (1881).

[122] *Id.* at 338.

[123] *Id.* at 336.

[124] 17 U.S.C. § 106 (2012) (stating that "the owner of copyright under this title has the exclusive rights" to perform, display, and distribute copies of the work to the public).

[125] *Id.* § 101.

[126] 749 F.2d 154 (3d Cir. 1984).

public constituted a "public performance."[127] The court noted that the definition in the statute of public performance:

> is written in the disjunctive, and thus two categories of places can satisfy the definition of "to perform a work publicly." The first category is self-evident; it is "a place open to the public." The second category, commonly referred to as a semi-public place, is determined by the size and composition of the audience.[128]

Like other conceptualizations, accessibility seems to be a key component to this conceptualization.[129]

e. *Open For Business*

Some statutes evoke the notions of public accessibility for commerce, both in terms of access to premises as well as the intended audience for marketing efforts. For example, Idaho's "ag-gag" law prohibits entering "an agricultural production facility that is not open to the public and, without the facility owner's express consent . . . , mak[ing] audio or video recordings of the conduct of an agricultural production facility's operations . . . ."[130]

In *Flytenow, Inc. v. Federal Aviation Administration*,[131] the D.C. Circuit Court of Appeals addressed the Federal Aviation Administration interpretation that Flytenow—a ridesharing service for flights—was "holding out to the public" in such a way as to constitute a commercial service.[132] While the court did not define the relevant "public," it stated that "[a]ny prospective passenger searching for flights on the Internet could readily arrange for travel via Flytenow.com."[133] Although Flytenow required prospective passengers to hold a Flytenow membership in order to use the platform, the court nonetheless found that Flytenow pilots were holding out to the public because "membership require[d] nothing more than signing up."[134] Although not explicitly stated by

---

[127] *Id.* at 156.

[128] *Id.* at 158.

[129] *Id.* As the court stated:

> The legislative history indicates that this second category was added to expand the concept of public performance by including those places that, although not open to the public at large, are accessible to a significant number of people. Clearly, if a place is public, the size and composition of the audience are irrelevant. However, if the place is not public, the size and composition of the audience will be determinative.

Id. (emphasis added) (citation omitted) But this statement conflicts with the fact that the very definition of what is public is often dependent upon the size and composition of an audience.

[130] IDAHO CODE § 18-7042(1)(d) (2018). For more information on laws that restrict information collection, see generally Margot E. Kaminski, *Privacy and the Right to Record*, 97 B.U. L. REV. 167 (2017).

[131] 808 F.3d 882 (D.C. Cir. 2015).

[132] *Id.* at 893.

[133] *Id.* at 892.

[134] *Id.*

the court, it essentially concluded that Flytenow pilots were holding out to the public based on the fact that virtually anyone using the Internet could access information posted by pilots on Flytenow's website, regardless of whether or not anyone actually accessed the information.

f. *Publication and Publicity*

What constitutes a "publication" and "publicity" for legal purposes derives from the concept of the "public." Accordingly it is not surprising that the concept of publication struggles with the same inconsistencies inherent in the concept of public information, notably the difference between accessibility and knowledge. The term "publish" is defined as "to *make generally known*" or "to disseminate to the public."[135] But to publish is to engage in "publication," which is defined as "the act or process of producing a book, magazine, etc., and *making it available* to the public."[136] Again we see the difference between theoretical availability and effective dissemination and cognition.

Courts, scholars, policy makers, and academics have debated how to define the concept of publication. In patent law, the "printed publication" bar hinges upon a finding of "public accessibility."[137] In Part III, I will argue that the major importance of an accessibility conceptualization over a knowledge-based one is that accessibility requires no proof that anyone ever actively received, read, or understood information.[138]

In copyright law, § 101 of the Copyright Act states that:

> "Publication" is the *distribution* of copies or phonorecords of a work to the public by sale or other transfer of ownership, or by rental, lease, or lending. The *offering* to distribute copies or phonorecords to a group of persons for purposes of further distribution, public performance, or public display, constitutes publication. A public performance or display of a work does not of itself constitute publication.[139]

In *London-Sire Records, Inc. v. Doe 1*,[140] the district court provided an extensive discussion regarding whether the term "publication" is synonymous

[135] *Publish*, MERRIAM-WEBSTER'S COLLEGIATE DICTIONARY, *supra* note 110 (emphasis added).

[136] *Publication*, MERRIAM-WEBSTER'S COLLEGIATE DICTIONARY, *supra* note 110 .

[137] *See, e.g.*, *In re* Klopfenstein, 380 F.3d 1345, 1349 (Fed. Cir. 2004); *In re* Hall, 781 F.2d 897, 899 (Fed. Cir. 1986) (calling public accessibility the "touchstone" for printed publication determinations).

[138] *See infra* Part III (describing different conceptualizations of privacy).

[139] 17 U.S.C. § 101 (2012) (emphasis added).

[140] 542 F. Supp. 2d 153 (D. Mass. 2008).

for "distribution."[141] While "distribution" is left undefined by copyright statutes, the court referred to the portion of § 101 quoted above.

Thus, it seems that if someone offers or in fact effectively distributes something, even to possibly one person, they have "published" it. Section 106(3) of the Copyright Act grants the copyright holder an exclusive right "to distribute copies . . . of the copyrighted work to the public . . . ."[142] In *Ford Motor Co. v. Summit Motor Products, Inc.*,[143] the Third Circuit Court of Appeals concluded that "even one person can be the public for the purposes of Section 106(3)."[144] However, in *Cartoon Network LP v. CSC Holdings, Inc.*,[145] the Second Circuit Court of Appeals held that RS-DVR playback transmissions "are not performances 'to the public,'" and accordingly do "not infringe any exclusive right of public performance," based on the fact that such transmissions are "made to a single subscriber using a single unique copy produced by that subscriber . . . ."[146]

What constitutes a "public performance" is also debatable. The Copyright Act provides that performing a work publicly means "to perform . . . it at a place *open to the public* or at any place where a *substantial* number of persons outside of a normal circle of a family and its social acquaintances *is gathered*."[147] In *Columbia Pictures Industries, Inc.*, the Third Circuit Court of Appeals recognized that a § 101 category of place, "commonly referred to as a semi-public place, is determined by the size and composition of the audience."[148]

With regard to this second category, "[t]he legislative history indicates that [it] was added to expand the concept of public performance by including those places that, although not open to the public at large, are accessible to a significant number of people."[149] Here again there are two possible notions of what constitutes public: the mere possibility of a public grouping or an actual gathering of people. This tension between hypotheticals and reality exists in nearly every legal conceptualization of public. As I will discuss in Part II, this distinction is critical for privacy law, yet it is rarely clear which notion is

[141] *Id.* at 165-75 ("By the plain meaning of the statute, all 'distributions . . . to the public' are publications. But not all publications are distributions to the public—the statute explicitly creates an additional category of publications that are not themselves distributions.").

[142] 17 U.S.C. § 106(3).

[143] 930 F.2d 277 (3d Cir. 1991).

[144] *Id.* at 299.

[145] 536 F.3d 121 (2d Cir. 2008).

[146] *Id.* at 139.

[147] 17 U.S.C. § 101 (emphasis added).

[148] Columbia Pictures Indus., Inc. v. Redd Horne Inc., 749 F.2d 154, 158 (3d Cir. 1984). Is the concept of "open to the public" really self-evident? When do things like membership restrictions become burdensome enough to change the status of a public business to a private club?

[149] *Id.* (citing H.R. REP. NO. 94-1476, at 64 (1976)).

intended in the rules. And to the extent legal regimes equate public information with hypothetically accessible information, they are misguided.

B. *The Discourse of Public Information*

There is a powerful assumption built into many of our modern conversations about privacy: if anyone can hypothetically access or view you and your data, then anyone can use it. In other words, if you put something "out there" for people to see, you should not complain when people collect, use, and share it. For example, in responding to people's concerns about the large amount of publicity given to peoples' tweets discussing their own sexual assault stories, Hamilton Nolan wrote in a column for *Gawker*:

> The things you write on Twitter are public. They are published on the world wide web. They can be read almost instantly by anyone with an internet connection on the planet Earth. This is not a bug in Twitter; it is a feature. Twitter is a thing that allows you to publish things, quickly, to the public.
>
> Most things that you write on Twitter will be seen only by your followers. Most things that you write on Twitter will not be read by the public at large. But that is only because the public at large does not care about most things that you have to say. It is not because the public does not have "a right" to read your Twitter. Indeed, they do. They can do so simply by typing Twitter dot com slash [your name] into their web browser. There, they will find a complete list of everything that you have chosen to publish on Twitter, which is a public forum.[150]

To Nolan and many others, hypothetical accessibility is what determines whether something is public. If anyone with an Internet connection *could* possibly access the information, then, the argument goes, your complaints for downstream use and bringing more attention to your disclosures are unjustified. Nolan's public/private dichotomy underscores the ability to control the accessibility of tweets. He wrote, "If you do not want your Twitter to be public, you can make it private. Then it will not be public. If you do not make it private, it will be public." [151]

Nolan is hardly alone in this sentiment. Many in industry, the media, the advocacy community, and society-at-large regularly argue that if it is accessible, it is public. For example, Hannah McGill wrote in an op-ed in *The Scotsman* about the publicness of online interaction:

---

[150] Nolan, *supra* note 16. Nolan was responding to privacy concerns raised by the aggregation of tweets into a story on *Buzzfeed* describing what people were wearing when they were sexually assaulted. For the *Buzzfeed* story, see Jessica Testa, *Sexual Assault Survivors Answer the Question "What Were You Wearing When You Were Assaulted?,"* BUZZFEED (Mar. 12, 2014, 11:42 PM), https://www.buzzfeed.com/jtes/sexual-assault-survivors-answer-the-question-what-were-you-w [https://perma.cc/ABB8-KTGA].

[151] Nolan, *supra* note 16.

> You can't place stuff in the public domain and then feel hunted or betrayed if it's slyly traced back to you using underhand techniques like – er - reading the name on your profile. How strange that putting someone's name in a newspaper is regarded as "naming and shaming" whereas shaming yourself publicly still seems to fall within most people's conception of private communication.[152]

Google responded to privacy concerns over its data collection for its "Street View" feature, saying "Street View only features imagery taken on public property. . . . This imagery is no different from what any person can readily capture or see walking down the street."[153] Jeff Jarvis, a prominent journalism professor and author, has identified himself as an advocate of "publicness," which he defined as "1. The act or condition of sharing information, thoughts, or actions. 2. Gathering people or gathering around people, ideas, causes, needs: 'Making a public.' 3. Opening a process so as to make it collaborative. 4. An ethic of openness."[154] Professor Jarvis, like many, sees public and private as flip sides of a coin, with the implication being they are mutually exclusive. He wrote, "Private and public are choices we make: to reveal or not, to share or not, to join or not" and went on to define the Internet as "our new public place."[155]

Nissenbaum noted the common response to people who claim privacy in public:

> [W]hen people move about and do things in public arenas, they have implicitly yielded any expectation of privacy. Much as they might *prefer* that others neither see, nor take note, *expecting* others not to see, notice, or make use of information so gained would be unreasonably restrictive of others' freedoms. One cannot reasonably insist that people avert their eyes, not look out their windows, or not notice what others have placed in their supermarket trolleys. And if we cannot stop them from looking, we cannot stop them remembering and telling others. In 2001, Tampa police, defending their use of video cameras to scan faces one-by-one as they entered the Super Bowl stadium, stated, "the courts have ruled that there is no expectation of privacy in a public setting."[156]

---

[152] Hannah McGill, *No Privacy when Personal Opinion Is Posted in Public*, SCOTSMAN (Nov. 22, 2015, 12:01 AM), http://www.scotsman.com/lifestyle/culture/hannah-mcgill-no-privacy-when-personal-opinion-is-posted-in-public-1-3955011 [https://perma.cc/4ENA-4Q6U] ("The fact that the individuals who posted angry messages have been identified in the media – not only by their names, but by their places of work – has been decried by some as witch hunting and scare tactics. And yet the press didn't expose them: they exposed themselves.").

[153] Miguel Helft, *Google Photos Stir a Debate over Privacy*, N.Y. TIMES, June 1, 2007, at C1.

[154] JEFF JARVIS, PUBLIC PARTS 1 n.* (2011).

[155] *Id.* at 8.

[156] Nissenbaum, *supra* note 86, at 135-36.

The common story we tell ourselves about public information matters, because it frames our norms and policies.[157] When we endow the descriptive conceptualization of public information with exculpatory power, we legitimize certain kinds of behaviors.

While some scholars generally agree with the "no privacy in public" sentiment,[158] others have long critiqued the idea that there is no privacy in public.[159] Professor Joel Reidenberg argued that "[t]he recreation of privacy in public suggests that the 'reasonable expectation of privacy' standard needs to

[157] *See, e.g.*, Woodrow Hartzog, *supra* note 31, at 1021 ("[E]ven small changes in the presentation of an issue or event can produce significant changes of opinion.").

[158] *See, e.g.*, 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 (2012) ("[T]his Article concludes that the law should not restrict the collection and reporting of truthful information shared in public in order to prevent a perceived, potential harm to someone's privacy interests."); Kirtley, *supra* note 69, at 97 ("If the records are public -- and presumptively a matter of public interest - at their source, that interest does not fade away simply because the records have been consolidated in one place."); Robert G. Larson III, Note, *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, 112 (2013) ("The marketplace of ideas theory is fundamentally at odds with the notion that one has a *privacy* interest in matters that have already been exposed to the public.").

[159] *See, e.g.*, Erin B. Bernstein, *Health Privacy in Public Spaces*, 66 ALA. L. REV. 989, 993 (2015) ("[B]oth courts and scholars . . . rejected for the most part claims to privacy for actions undertaken in public spaces. Such rejections are often based on the idea that, simply by being in public spaces, individuals consent to being recorded. But it cannot be said that individuals seeking health care services are moving through public spaces entirely voluntarily." (footnotes omitted)); Marc Jonathan Blitz, *The Fourth Amendment Future of Public Surveillance: Remote Recording and Other Searches in Public Spaces*, 63 AM. U. L. REV. 21, 43 (2013) ("In short, if public and visible space remains a Fourth Amendment-free zone, it provides . . . [police] with unlimited space to record, track, and review the minute-by-minute activities of individuals they have no reason to suspect of a crime."); Andrew Guthrie Ferguson, *Personal Curtilage: Fourth Amendment Security in Public*, 55 WM. & MARY L. REV. 1283, 1292 (2014) ("[P]ersons in public should be able to carve out constitutionally protected areas secure from government surveillance. This constitutionally protected area may be limited, but it exists." (footnote omitted)); Rachel Levinson-Waldman, *Hiding in Plain Sight: A Fourth Amendment Framework for Analyzing Government Surveillance in Public*, 66 EMORY L.J. 527, 530 (2017) ("Existing case law, seen through a new lens, provides the blueprint for a workable, comprehensive mechanism for applying the Fourth Amendment to digital age public surveillance technologies."); Diane L. Zimmerman, *Requiem for a Heavyweight: A Farewell to Warren and Brandeis's Privacy Tort*, 68 CORNELL L. REV. 291, 347 (1983) (criticizing idea that location of action can determine public or private nature); Josh Blackman, Note, *Omniveillance, Google, Privacy in Public, and the Right to Your Digital Identity: A Tort for Recording and Disseminating an Individual's Image over the Internet*, 49 SANTA CLARA L. REV. 313, 358 (2009) (stating that laws requiring several feet of space between paparazzi and victims "serve as an important step towards recognizing privacy in public, eschewing with the binary *Restatement* approach, and are an important basis for the first element of the right to your digital identity").

give way to a standard that takes into consideration [a distinction] between observable acts that are 'non-public,' or private-regarding, and those that are of public significance, or 'governance-related.'"[160] Other scholars challenge that a binary distinction between public and private even exists. For example. Nissenbaum and others have publicly criticized the idea of an overly-simplistic "public/private" dichotomy.[161] Professor Andrew McClurg argued that "[p]rivacy is a matter of degree. . . . There is a difference, which the law should recognize, between being 'seen' in public and being closely scrutinized or . . . recorded on film or videotape."[162] Professor Diane Zimmerman criticized using factors like "location" as principles of distinction to identify public and private places.[163] Professor Julie Cohen also leveled a critique of how notions of

[160] Reidenberg, *supra* note 22, at 155.

[161] HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE 89-100 (2010) ("[T]he line dividing public and private . . . is neither static nor universal."); *see also* Gary T. Marx, *Murky Conceptual Waters: The Public and the Private*, 3 ETHICS & INFO. TECH. 157, 157 (2001) (arguing that public/private distinction should be treated "as multi-dimensional, continuous and relative, fluid and situational or contextual, whose meaning lies in how [it is] interpreted and framed"); Frederick Schauer, *Internet Privacy and the Public-Private Distinction*, 38 JURIMETRICS 555, 558 (1998) ("[W]e must consider that the Internet would present a danger to privacy if the Internet only increased the ease and thus the frequency of access to otherwise private information, even if such information was previously accessible, but accessed only rarely."); Andrew D. Selbst, *Contextual Expectations of Privacy*, 35 CARDOZO L. REV. 643, 647 (2013) ("Specific definitions of 'private' and 'public,' however, differ depending on who is asked, and in what context."); Anne W. Branscomb, The Economics of Information: Public and Private Domains of Information: Defining the Legal Boundaries, Keynote Address at the 1994 ASIS Annual Meeting (Oct. 17, 1994). Nissenbaum's theory of contextual integrity has been influential as an alternative to more rigid articulations of privacy and public. *See, e.g.*, Alexis C. Madrigal, *The Philosopher Whose Fingerprints Are All over the FTC's New Approach to Privacy*, CTIONARY (Mar. 29, 2012), https://www.theatlantic.com/technology/archive/2012/03/the-philosopher-whose-fingerprints-are-all-over-the-ftcs-new-approach-to-privacy/254365/ ("[Nissenbaum] played a vital role in reshaping the way our country's top regulators think about consumer data.").

[162] Andrew Jay McClurg, *Bringing Privacy Law Out of the Closet: A Tort Theory of Liability for Intrusions in Public Places*, 73 N.C. L. REV. 989, 1041 (1995).

[163] Zimmerman wrote:

> First, what is a public place? For example, suppose that a tort claim is based on the allegation that the press has unjustly revealed that the plaintiff is a cocaine user. If a reporter obtained that information by watching the plaintiff use the drug on a park bench or a public street corner, courts generally agree that the reporter invades no right of privacy by revealing what he or she has seen. But the plaintiff's use of the same drug in a private club, at a large house party before fifty guests, or even in an intimate gathering of a few friends, poses logical difficulties for the location test. In each case, the plaintiff acted in view of others. A reporter may be present, or one of the guests may describe the behavior to others including the reporter who writes of it. In some senses, all these scenarios involve public action on the plaintiff's part. It is not clear, however, which of

publicness are used to justify information practices like surveillance. Cohen wrote, "Contemporary practices of personal information processing constitute a new type of public domain, which I will call the *biopolitical public domain*: a repository of raw materials that are there for the taking and that are framed as inputs to particular types of productive activity."[164] Cohen also critiqued the related concept of "visibility," writing that "focusing on visibility diminishes the salience and obscures the operation of nonvisual mechanisms designed to render individual identity, behavior, and preferences transparent to third parties. The metaphoric mapping to visibility suggests that surveillance is simply passive observation rather than the active production of categories, narratives, and norms."[165]

My argument in this Article is in the same spirit as these critiques. While many of these arguments are focused on the existence of privacy in public, my target is the concrete existence of a public itself. Specifically, I am critiquing the assumptions made about the public nature of information and its endowment as a deterministic category in privacy law and policy. To move forward, we must reject this assumption and clarify what is meant by "public" information and acts. In the next part, I look to the body of law and relevant discourse to map out three possible ways to conceptualize public information. Each of them have unique costs, benefits, ambiguities, and optimal uses.

II. THERE ARE THREE WAYS TO CONCEPTUALIZE PUBLIC INFORMATION

The problem with public information in the law is that it can be defined a few different ways, and it is not clear in many contexts which definition is meant. If public information is defined too broadly, it will include many different kinds of acts and information in which people might have some legitimate privacy interest. If the concept of public information is left ambiguous, those who seek to validate surveillance and data practices can use the normative and legal appeal of publicness without having to meaningfully defend the categorization.

The standard dictionary definition for "public" is deceptively simple. *Black's Law Dictionary* defines the adjective as "1. Of, relating to, or involving an entire community, state, or country. 2. Open or available for all to use, share, or enjoy."[166] As a noun, the term public is defined as "1. The people of a nation or community as a whole <a crime against the public>. 2. A place open or visible to the public <in public>."[167]

---

these sites are "public" places. It is also not clear what weight that distinction should carry in imposing liability.

Zimmerman, *supra* note 159, at 347 (footnote omitted).

[164] Cohen, *supra* note 35, at 214.

[165] Julie E. Cohen, *Privacy, Visibility, Transparency, and Exposure*, 75 U. CHI. L. REV. 181, 181 (2008).

[166] *Public*, BLACK'S LAW DICTIONARY (10th ed. 2014).

[167] *Id. Merriam-Webster*'s definition demonstrates the many different ways "public" can be defined, with significant differences between the conceptualizations:

A closer look of this definition shows why public is a complex construct. Even if information is observable or accessible, that does not necessarily mean that it is socially acceptable for all to share, use, or enjoy. Also, what is meant by "open or available"? Structurally exposed? Normatively inclusive? Legally permissible physical presence? And who is meant by the "all" in "open and available" to all? A few passersby might be able to catch a fleeting glimpse of an exposed undergarment or compromising position, yet that same piece of information would hardly seem to extend to "all to share, use, or enjoy" both as a practical and normative matter. But if "all" is an entire community, does that mean only what is actually or hypothetically visible to anyone in a community? And did you notice *Black's Law Dictionary* used the term "public" to define what is "public"?[168]

I should be careful to point out that I am not taking issue with the term public to the extent it is used to mean government or quasi-government entities or activities, such as "public sector" or "public law" or "public school." There might be grey areas within these notions,[169] but it is relatively clear in most instances who the government actors are. Nor am I concerned with the term "public" when it is used to generally modify terms like "public policy" or the specific meaning of "public utility." Also general, umbrella terms that act as shorthand for complex concepts can be quite useful in certain contexts. Terms like "privacy" and "big data" work in similar ways. But we should be more specific when it comes to defining rights and obligations.[170] Finally, I do not

> 1 a : exposed to general view : open
> b : well-known, prominent
> c : perceptible, material
> 2 a : of, relating to, or affecting all the people or the whole area of a nation or state . . .
> b : of or relating to a government
> c : of, relating to, or being in the service of the community or nation
> 3 a : of or relating to people in general : universal
> b : general, popular
> 4 : of or relating to business or community interests as opposed to private affairs: social
> 5 : devoted to the general or national welfare : humanitarian
> 6. a : accessible to or shared by all members of the community . . . .

Public, MERRIAM-WEBSTER'S COLLEGIATE DICTIONARY, *supra* note 110.

[168] *Public*, BLACK'S LAW DICTIONARY, *supra* note 166 (defining public as "place open or visible to the public").

[169] *See, e.g.*, Marsh v. Alabama, 326 U.S. 501, 502 (1946) (deciding "whether a State . . . can impose criminal punishment on a person who undertakes to distribute religious literature on the premises of a company-owned town contrary to the wishes of the town's management").

[170] The notion of "reasonable expectation of privacy" suffers from a similar problem. *See* Solove, *supra* note 25, at 1512-13 ("For a long time, I believed that with the appropriate understanding of privacy—one that is well-adapted to modern technology, nimble and nuanced, forward-looking and sophisticated—Fourth Amendment jurisprudence could be

wish to pick a fight with legal terms of art that already have exacting and refined contours such as "public figures" and "public forums." My critique lies with treating public information as though it were part of an objectively measured map capable of easily divided up by metes and bounds.

In Part I, I described how the concept of public information is deployed in various legal regimes often with little clarification.[171] Now, I map out three different conceptualizations of public information: (1) descriptive of content and context; (2) anything that is "not private"; and (3) designated for collection, use, and disclosure. While the boundaries of these concepts can overlap, they are generally discernable.

Importantly, these conceptualizations can have significantly different effects when implemented. Thinking of "public" as a description reduces determinations of people's privacy down to an empirical appeal. To determine one's privacy rights, you need only check to see if you are "in public" or if the data was "publicly available." Thinking of "public" as "not private" means you simply have to answer a different question—what is private? And thinking of public as a designation for information to collect, share, and use means a process must be established by the relevant authority to determine which pieces of information should be made public and under what circumstances.

In many legal regimes, it is unclear which conceptualization governs or should govern. The result is inconsistent and conflicting rules about when information becomes public. At their worst, legal regimes sacrifice nuance and even policy goals by drawing easy descriptive lines at the disclosure of information. The rationale is that once information is shared with others, it is public. I will argue in Part III that we need better, more nuanced notions of public information that recognize it as an exercise of power, not an overly simplified, purportedly objective, description of shared information.[172]

A. *Descriptive of Context or Content*

The default notion of public information in law and society seems to be descriptive of the context in which the information was shared. When people say there is no privacy "in public" or that data is "already public," they most plausibly seem to be describing an attribute or context of the act or information.[173] Descriptive factors such as who the information was shared with,

rehabilitated. I now realize I was wrong. The entire debate over reasonable expectations of privacy is futile, for it is not focused on the right question.").

[171] *See supra* Section I.A (describing different legal concepts in which privacy is material issue).

[172] NEIL RICHARDS, INTELLECTUAL PRIVACY: RETHINKING CIVIL LIBERTIES IN THE DIGITAL AGE 166 (2015) ("Sharing information with a few other people doesn't make it public; it just makes it information.").

[173] Here, the word "in" is likely being used as a preposition describing information or acts surrounded by or enclosed in "public" and the word "is" is likely being used to describe a state of being.

how many people were actually exposed to certain acts, how many people actually saw and internalized information, where the acts occurred, where the information was located, and any particular barriers to access or dissemination are all relevant to articulate what is public.[174] Zimmerman noted, "To distinguish private facts from 'public' information about an individual, courts often look either to the location of the action or to the nature of the subject matter. Courts using the 'location' analysis commonly state that information individuals reveal about themselves in public places is by definition not private."[175] Professor Patricia Sanchez Abril has observed that the privacy torts looked to core descriptive concepts of space, subject matter, secrecy, and seclusion to define the scope of privacy rights.[176] These descriptive concepts have basically served as proxies for the dividing line between public and private.[177] A review of the law and literature reveals there are at least three different popular descriptive accounts of "public" used in legal regimes: accessible, known, and "of interest to society."

[174] *See, e.g.*, Richard G. Wilkins, *Defining the "Reasonable Expectation of Privacy": An Emerging Tripartite Analysis*, 40 VAND. L. REV. 1077, 1122 (1987) ("Despite an individual's most ardent desires, society and the courts realistically cannot recognize certain information as 'private' in any real sense of the word. Such information includes a person's own physical characteristics—appearance, height, weight, and, in most cases, gender—which simply cannot be shielded from the public gaze. The Supreme Court has concluded that this category of inherently 'public' information includes fingerprints and the physical characteristics of the voice itself. Furthermore, while a person's 'papers' are entitled to explicit constitutional protection, the actual vehicle of written communication—namely, an individual's handwriting—is not 'private' within the meaning of the fourth. 'Handwriting, like speech, is repeatedly shown to the public, and there is no more expectation of privacy in the physical characteristics of a person's script than there is in the tone of his voice.'").

[175] Zimmerman, *supra* note 159, at 347 (citing Gill v. Hearst Publ'g Co., 253 P.2d 441, 444 (Cal. 1953); then citing Metter v. L.A. Examiner, 95 P.2d 491, 496 (Cal. 1939); then citing Jacova v. S. Radio & Television Co., 83 So. 2d 34, 40 (Fla. 1955); then citing Forster v. Manchester, 189 A.2d 147, 150 (Pa. 1963); then citing RESTATEMENT (SECOND) OF TORTS § 652D cmt. b (AM. LAW INST. 1977)).

[176] Abril, *supra* note 22, at 4.

[177] *Id.* at 6-18 ("[C]ourts have generally held that anything capable of being viewed from a 'public place' does not fall within the privacy torts' protective umbrella. . . . Under the Restatement, an individual cannot have a reasonable expectation of privacy in any public place. More formally, any activity that is visible to the public eye—whether that eye is human or mechanical—is not actionable under the public disclosure tort. For example, courts have found that there is no reasonable expectation of privacy in a restaurant, in a church service, or at a county fair." (citing RESTATEMENT (SECOND) OF TORTS § 652D cmt. b (AM. LAW INST. 1977); then citing Wilkins v. NBC, 84 Cal. Rptr. 2d 329 (Cal. Ct. App. 1999); then citing Creel v. I.C.E. & Assocs., Inc., 771 N.E.2d 1276 (Ind. Ct. App. 2002); then citing Daily Times Democrat v. Graham, 162 So. 2d 474, 476 (Ala. 1964))).

1. Freely Accessible

The most common descriptive conceptualization of public information within the law seems to be any information that is hypothetically or "freely" accessible. It is the way the dictionary describes "public."[178] It is often the colloquial use.[179] And most importantly for law and policy, it is the way that notions of public are described in statutes, case law, and other doctrinal sources.[180] The freely accessible conceptualization of public also creates the most problems for privacy.

The most important trait of public as "freely accessible" is that it is not contingent upon how many people have *actually* accessed or were cognizant of information, but rather either how hypothetically difficult it would be for people or just one person to access information or for others to be geographically close enough to be exposed to a person's acts.[181] Cognition of information is irrelevant. It is an exercise in conjecture.

The idea of hypothetical accessibility explicitly underlies the "plain view" doctrine, which exempts objects that are immediately apparent to officers lawfully present in a place where evidence can be plainly viewed from the warrant requirements of the Fourth Amendment.[182] In order to determine if something can be "plainly viewed," courts often ask whether any hypothetical member of the public could have seen an object or act without trespass or hardship. For example, the Supreme Court in *California v. Ciraolo*[183] focused on the fact that "any member of the public flying in this airspace who cared to glance down *could have* seen everything that the officers observed" in holding

[178] *See supra* Part II (positing three ways to conceptualize public information as descriptive, anything that is not "private," and official designation).

[179] *See supra* Section I.A.2 (describing concept of no reasonable expectation of privacy in a public place).

[180] *See supra* Section I.A.1 (summarizing intersection of tort law and notions of "public information").

[181] *Publication of Private Facts*, DIGITAL MEDIA L. PROJECT, http://www.dmlp.org/legal-guide/publication-private-facts [https://perma.cc/R4UK-FAR4] (last visited Feb. 15, 2019) ("A plaintiff has no privacy interest with respect to a matter that is already public. Thus, you cannot be held liable for discussing or republishing information about someone that is already publicly available (e.g., found on the Internet or in the newspaper)."); *see* Cohen, *supra* note 165, at 190 ("[T]he interesting thing about the reasonable expectations test is that it is fundamentally concerned not with expectations about the nature of particular *spaces*, but rather with expectations about the accessibility of *information* about activities taking place in those spaces.").

[182] Horton v. California, 496 U.S. 128, 134-37 (1990) (describing scope of "plain view" doctrine); United States v. Legg, 18 F.3d 240, 242 (4th Cir. 1994) (summarizing three conditions of "plain view" doctrine as: officers are lawfully in a place from which the evidence can be plainly viewed, officers have legal right of access to the object, and object's "incriminating character" must be apparent).

[183] 476 U.S. 207 (1986).

that the Fourth Amendment did not apply to the search.[184] In *California v. Greenwood*,[185] the Court concluded that "respondents exposed their garbage to the public sufficiently to defeat their claim to Fourth Amendment protection. It is common knowledge that plastic garbage bags left on or at the side of a public street are *readily* accessible to animals, children, scavengers, snoops, and other members of the public."[186]

The Court in *Greenwood* seemed to equate making something freely accessible with the waiver of privacy rights, holding that "respondents placed their refuse at the curb for the express purpose of conveying it to a third party, the trash collector, who might himself have sorted through respondents' trash or permitted others, such as the police, to do so."[187] As a result of "having deposited their garbage 'in an area particularly suited for public inspection and, in a manner of speaking, public consumption, for the express purpose of having strangers take it,'" the Court found that the defendants had no reasonable expectation of privacy in the inculpatory items they threw out in the trash.[188]

In *United States v. Knotts*,[189] the Supreme Court similarly held that "[a] person travelling in an automobile on public thoroughfares has no reasonable

[184] *Id.* at 208 (emphasis added) ("The Fourth Amendment simply does not require police traveling in the public airways at 1,000 feet to obtain a warrant in order to observe what is visible to the naked eye.").

[185] 486 U.S. 35 (1988).

[186] *Id.* at 40 (emphasis added) ("[O]f those state appellate courts that have considered the issue, the vast majority have held that the police may conduct warrantless searches and seizures of garbage discarded in public areas." (citing Smith v. State, 510 P.2d 793, 795-95 (Ala. 1973); then citing State v. Fassler, 503 P.2d 807, 813-14 (Ariz. 1972); then citing State v. Schultz, 388 So. 2d 1326, 1329 (Fla. Dist. Ct. App. 1980); then citing People v. Huddleston, 347 N.E.2d 76, 80-81 (Ill. App. Ct. 1976); then citing Commonwealth v. Chappee, 492 N.E.2d 719, 721-22 (Mass. 1986); then citing People v. Whotte, 317 N.W.2d 266, 268-69 (Mich. Ct. App. 1982); then citing State v. Oquist, 327 N.W.2d 587, 591 (Minn. 1982); then citing State v. Ronngren, 361 N.W.2d 224, 228-30 (N.D. 1985); then citing State v. Brown, 484 N.E.2d 215, 217-18 (Ohio Ct. App. 1984); then citing Cooks v. State, 699 P.2d 653, 656 (Okla. Crim. App. 1985); then citing State v. Purvis, 438 P.2d 1002, 1005 (Or. 1968); then citing Commonwealth v. Minton, 432 A.2d 212, 217 (Pa. Super. Ct. 1981); then citing Willis v. State, 518 S.W.2d 247, 249 (Tex. Crim. App. 1975); then citing Smith v. State, 510 P.2d 793, 798 (Alaska 1973); then citing State v. Stevens, 367 N.W.2d 788, 794-97 (Wis. 1985); then citing Croker v. State, 477 P.2d 122, 125-26 (Wyo. 1970)); citing in contrast People v. Krivda, 486 P.2d 1262, 1268-69 (Cal. 1971) (holding defendant had reasonable expectation of privacy for trash that had not yet lost its "identity" by getting mixed with all municipal trash); then citing State v. Tanaka, 701 P.2d 1274, 1276-77 (Haw. 1985) (holding there is reasonable expectation of privacy in trash bags and that police will not enter private property to open trash bags)).

[187] *Id.* at 35.

[188] *Id.* at 40-41 (citing United States v. Reicherter, 647 F.2d 397, 399 (3d Cir. 1981)).

[189] 460 U.S. 276 (1983).

expectation of privacy in his movements from one place to another."[190] The rationale for the Court's reasoning is that when a person travels on public streets he voluntarily conveys "to anyone who want[s] to look the fact that he [is] traveling over particular roads in a particular direction, the fact of whatever stops he ma[kes], and the fact of his final destination when he exit[s] from public roads onto private property."[191]

The intrusion upon seclusion tort also largely exempts "public places" or things that are in "plain view" from its reach mainly because such places and things are freely accessible.[192] Electronic surveillance law also embraces the notion of public as freely accessible—sometimes quite explicitly. The Wiretap Act, which regulates the interception of electronic communication while in transit, explicitly exempts (and thus permits) the interception of communications that are "readily accessible to the general public."[193]

The freely accessible conceptualization of public information is also implicit in claims where exposure to others invalidates a privacy interest because "anyone could have seen you." This colloquial reference to hypothetical accessibility has been common in society since the turn of the nineteenth century.[194] It persists today. In *Daly v. Viacom, Inc.*,[195] the plaintiff brought a tort claim for public disclosure of private facts based on the defendants publicizing her kissing a man in a bathroom stall.[196] In rejecting the plaintiff's claim, the court noted that the plaintiff had already kissed the man in public and

[190] *Id.* at 281.

[191] *Id.* at 281-82.

[192] *See, e.g.*, Shulman v. Grp. W Prods., Inc., 955 P.2d 469, 490 (Cal. 1998) ("Cameraman Cooke's mere presence at the accident scene and filming of the events occurring there cannot be deemed either a physical or sensory intrusion on plaintiffs' seclusion. Plaintiffs had no right of ownership or possession of the property where the rescue took place, nor any actual control of the premises. Nor could they have had a reasonable expectation that members of the media would be excluded or prevented from photographing the scene . . . .").

[193] Wiretap Act, 18 U.S.C. § 2511(2)(g)(i) (2012); *see* Joffe v. Google, Inc., 746 F.3d 920, 925 (9th Cir. 2013).

[194] *See* Barbas, *supra* note 37, at 1002-03 ("We can see this 'no privacy in public' position as an attempt, albeit imprecisely, to describe the actual workings of the media in an age of photojournalism. It also reflected the somewhat ominous sense of media surveillance felt by much of the public at the time; life was often described as lived 'before the spotlight,' and 'the klieg lights spare nobody, high or low.' The normative rationale for the doctrine, as will be discussed, was rooted in concerns with freedom of the press. It was feared that a right to privacy in public places would exert an inhibitive effect on publishing, impairing the public's ability to access the news through the media of mass communications." (footnote omitted)); Hadley, *supra* note 39, at 11-12 ("When an individual . . . walks along the streets in the sight of all . . . , he has waived his right to the privacy of his personality.").

[195] 238 F. Supp. 2d 1118 (N.D. Cal. 2002).

[196] *Id.* at 1124.

in plain view, both in a bar and on a city sidewalk.[197] As a result, the fact that she had kissed this man was not private.[198]

The freely accessible view of public as a waiver of privacy rights was encapsulated bluntly by Judge Sciarrino in his decision rejecting any privacy interest in posts made on Twitter.[199] The judge wrote:

> If you post a tweet, *just like if you scream it out the window*, there is no reasonable expectation of privacy. There is no proprietary interest in your tweets, which you have now gifted to the world. This is not the same as a private email, a private direct message, a private chat, or any of the other readily available ways to have a private conversation via the Internet that now exist.[200]

In fact, the Internet has proven to be a poor fit for this notion of public information. Courts tend to treat information on the World Wide Web, that is accessed via a URL and does not require authentication credentials (like a username and password) as freely accessible.[201] This assumption applies whether the website in question is massively popular, like ESPN.com, or a random family blog or website dedicated to an extremely niche or obscure interest. That is because a hypothetical Internet user armed with the right web address or search terms could find the information. For example, in *United States v. Gines-Perez*,[202] the United States District Court for the District of Puerto Rico considered whether government accessing and downloading information from a website violated the defendant's right of privacy.[203] The court stated:

> [P]lacing information on the information superhighway necessarily makes said matter accessible to the public, no matter how many protectionist measures may be taken, or even when a web page is "under construction." . . . [I]t strikes the Court as obvious that a claim to privacy is unavailable to someone who places information on an indisputably, public medium, such as the Internet, without taking any measures to protect the information.

---

[197] *Id.*

[198] *Id.*

[199] People v. Harris, 949 N.Y.S.2d 590, 593 (Crim. Ct. 2012) ("There can be no reasonable expectation of privacy in a tweet sent around the world.").

[200] *Id.* at 595 (emphasis added). Though for those that study modern electronic surveillance, the notion of emails and direct messages as "private" might be so dubious as to elicit a snicker.

[201] Ashcroft v. ACLU, 535 U.S. 564, 605 (2002) (describing Internet as "unique forum for communication because information, once posted, is accessible everywhere on the network at once").

[202] 214 F. Supp. 2d 205 (D.P.R. 2002).

[203] *Id.* at 224 ("Finally, the Court addresses the contention that, by accessing and downloading information from an Internet site, the government violated Gines-Perez's right of privacy.").

> . . . A person who places information on the information superhighway clearly subjects said information to being accessed by every conceivable interested party. Simply expressed, if privacy is sought, then public communication mediums such as the Internet are not adequate forums without protective measures.[204]

In *Sandler v. Calcagni*,[205] the court noted that "[p]laintiff admits that she revealed her decision to seek psychological help during college on her *publicly accessible* myspace.com webpage. As a result, the second passage is not actionable as it does not reveal a private fact."[206] This argument seems to boil down to the fact that passwords make things private, but absent that, everything on the World Wide Web is public because it is hypothetically available to anyone with an Internet connection.

The notions of "accessibility" and "exposure" are used interchangeably to define "public" here and throughout the doctrine. But it is not clear that they are synonymous. The literal definition of exposure—"the condition of being presented to view or made known"—conflates hypothetical availability and cognition.[207] This sort of semantic ambiguity is at the heart of the public information fallacy and it matters because hypothetical realities are constructed through conjecture. This conjecture requires a host of assumptions about the pre-existing knowledge base, resources, motivations, and abilities of people who make up "the public." It requires assumptions about social norms, architectural restraints, and pedestrian and vehicle traffic regarding the environment of exposure. And it requires assumptions about the timing and the relative visibility, audibility, and comprehensibility of the acts to be surveilled or the data to be collected. There are no rules about how to arrive at these assumptions, which means that determining that something is "freely accessible" can be wildly inconsistent and is often no better than a guess.

2. Widely Known

Sometimes it is not availability or observability that defines what is public, but rather a significant threshold of peoples' actual cognition of information or acts. I call this the "widely known" conceptualization of public information. This is sometimes referred to as "broadly known," "effective dissemination,"

---

[204] *Id.* at 225 (emphasis omitted).

[205] 565 F. Supp. 2d 184 (D. Me. 2008).

[206] *Id.* at 197 (emphasis added).

[207] *Exposure*, MERRIAM-WEBSTER'S COLLEGIATE DICTIONARY, *supra* note 110. Cohen noted this problem as a wrongful focus on visibility, writing, "focusing on visibility diminishes the salience and obscures the operation of nonvisual mechanisms designed to render individual identity, behavior, and preferences transparent to third parties. The metaphoric mapping to visibility suggests that surveillance is simply passive observation rather than the active production of categories, narratives, and norms." Cohen, *supra* note 165, at 181.

"publicized," or simply "famous."[208] The focus of this definition is on what people actually found, saw, or understood.[209] Things that are a shared or common knowledge among a group of people can be said to be public information. Most people in the United States probably know that the Cubs finally won the World Series.[210] Many people know that Beyoncé and Jay-Z are married and have three children.[211] Within my own New England community, most people probably know that Tom Brady is a legendary quarterback for the New England Patriots. While it can be incredibly difficult to consistently determine the boundaries of what is widely known, it is an ascertainable concept. The hard part is understanding the threshold quantity of people in the know or the boundaries of the relevant community.

An interesting example of conceptualizing public as "broadly known" is *Sipple v. Chronicle Publishing Co.*[212] Oliver Sipple was near Sara Jane Moore on September 22, 1975, when she attempted to assassinate President Ford.[213] Sipple interfered with Moore's assassination attempt and was credited as a hero.[214] Some of the publications that covered Sipple's story revealed the fact that he was gay, which was unknown to many close to him, including his parents, brothers, and sisters.[215] Sipple brought a tort claim against these publications for public disclosure of private facts.[216] The California Court of Appeal upheld the dismissal of the claim on the grounds that Sipple's sexual orientation was not a private fact because he had made the information public by marching in gay parades, frequenting gay bars, and being named in gay magazines.[217]

The court began its rationale for this decision with the seemingly entrenched maxim that "there can be no privacy with respect to a matter which is already public or which has previously become part of the 'public domain'" and "there

[208] *See, e.g.*, Sipple v. Chronicle Publ'g Co., 201 Cal. Rptr. 665, 669 (Ct. App. 1984) (explaining that there is no liability for public disclosure of private facts when defendant publicizes information which is already public or information that has been left open to public).

[209] *Id.*

[210] *See* Carrie Muskat, *Holy Now! 108 Years Later, Cubs Best in World*, MLB.COM (Nov. 3, 2016), https://www.mlb.com/news/cubs-win-world-series-after-108-years-waiting/c-207995060 [https://perma.cc/5C7J-LR56].

[211] *See* Jen Juneau, *How Beyoncé and JAY-Z Took All Three Kids – Even Their Year-Old Twins – on Tour*, PEOPLE (June 22, 2018), https://people.com/parents/beyonce-jay-z-twins-daughter-blue-ivy-on-tour/ [https://perma.cc/TBV4-YQYB].

[212] 201 Cal. Rptr. 665, 669 (Ct. App. 1984).

[213] *See id.* at 666.

[214] *Id.*

[215] *Id.* at 667.

[216] *Id.*

[217] *Id.* at 671 ("In summary, appellant's assertion notwithstanding, the trial court could determine as a matter of law that the facts contained in the articles were not private facts within the purview of the law and also that the publications relative to the appellant were newsworthy.").

is no liability when the defendant merely gives further publicity to information about the plaintiff which is already public or when the further publicity relates to matters which the plaintiff *leaves open* to the public eye."[218] When explaining these statements, the court did not focus on hypothetical accessibility. Rather, it focused on the fact that many in the relevant communities *actually knew* about Sipple's sexual orientation. The court wrote:

> The undisputed facts reveal that prior to the publication of the newspaper articles in question appellant's homosexual orientation and participation in gay community activities *had been known* by hundreds of people in a variety of cities, including New York, Dallas, Houston, San Diego, Los Angeles and San Francisco. . . . In fact, appellant quite candidly conceded that he did not make a secret of his being a homosexual and that if anyone would ask, he would frankly admit that he was gay. In short, since appellant's sexual orientation was *already in public domain* and since the articles in question did no more than to give further publicity to matters which appellant left open to the eye of the public, a vital element of the tort was missing rendering it vulnerable to summary disposal.[219]

While there is some ambiguity caused by referring to information that "had been known" by hundreds and "left open to the eye of the public"—the accessibility/knowledge distinction—it appears that the court was largely persuaded by the fact that people actually knew Sipple was gay in determining that this information was in the "public domain."[220]

Some laws that turn on whether information is "nonpublic" also often seem to adopt the "widely known" conceptualization of "public." For example, in *Dirks v. SEC*,[221] the Justice Blackmun in dissent stated that parties with inside information cannot trade based on such information unless they disclose it to the public.[222] For this sort of "public disclosure," the SEC requires more than mere disclosure to purchasers or sellers. It has indicated "[p]roper and adequate disclosure of significant corporate developments can only be effected by a public release through the appropriate public media, designed to achieve a *broad dissemination* to the investing public generally and without favoring any special person or group."[223] However, the Court did not provide examples of things that met this standard, and further, the SEC and the Court left undefined the term "public" as applied in this definition. Notions of whether people *actually*

[218] *Id.* at 678-79 (emphasis added) (citations omitted).

[219] *Id.* at 669 (emphasis added).

[220] *Id.*

[221] 463 U.S. 646 (1983).

[222] *Id.* at 678 (Blackmun, J. dissenting) ("The Commission tells persons with inside information that they cannot trade on that information unless they disclose [to the public].").

[223] Certain Trading in the Common Stock of Faberge, Inc., 45 SEC Docket 249, 256 (1973) (emphasis added).

accessed, heard, or otherwise were cognizant of information also seems embedded in the common law waiver of things like spousal privileges.[224]

Some conceptualizations of "public" combine "accessible" and "well-known" in a sort of "either-or" test. For example, the guidance provided by the Office of Information Policy in the U.S. Department of Justice, provides that "[u]nless the information has become 'practically obscure' . . . there is generally no expectation of privacy regarding information that is particularly *well known* or is *widely available* within the public domain."[225] Trade secret law has developed the "known" concept as well, whereby some information would not be protected as a trade secret if it is either "generally known" or "readily ascertainable." Trade secret scholars call this the "known/knowable" distinction."[226] Professor Sharon Sandeen has written that with respect to trade secret law:

> What is generally known is broadly defined to include what is known to the general public and what is known within discrete industries or groups of individuals who are experts in the field. Information is readily ascertainable if, even though it is not generally known, it can be found without much time, trouble or expense.[227]

As a descriptive account of public information, the "widely known" conceptualization of "privacy" seems more defensible than the "freely accessible" conceptualization because it generally requires less speculation and fewer assumptions. And while the general concept of privacy includes more than just secrets, to the extent the law does turn on secrecy, doing so based on what people actually know rather than hypothetical access seems more likely to match the expectations of those disclosing information and lead to a more consistent line in the sand to cut off privacy interests.

3. Of Interest to Society

A final, significant way to describe public information is as that which is "of interest to society." The focus of this conceptualization is not whether people can access information or whether they actually know it, but rather whether it is the kind of information that a significant part of society *would be* interested in accessing and knowing. Another version of this notion of public information adds a normative component, which defines the concept as that which is of

---

[224] *See* Williams v. State, 71 So. 3d 196, 198 (Fla. Dist. Ct. App. 2011) (holding husband's street name not privileged because it was generally known the community); Annotation, *supra* note 101.

[225] U.S. DOJ, DOJ GUIDE TO THE FREEDOM OF INFORMATION ACT OFFICE OF INFORMATION POLICY GUIDANCE: EXEMPTION 6, at 435 (2014) (emphasis added).

[226] *See* Sharon K. Sandeen, *Relative Privacy: What Privacy Advocates Can Learn from Trade Secret Law*, 2006 MICH. ST. L. REV. 667, 697.

[227] Sharon K. Sandeen, *Knowing What Is Known and Knowable*, PATENTLY-O (Sept. 3, 2014), http://patentlyo.com/patent/2014/09/guest-knowing-knowable.html [https://perma.cc/RWU2-AT6U] ("Among trade secret scholars, we say that the difference is between what is 'known' to the public and what is 'knowable.'").

"legitimate" interest to society, about which society *should* be concerned. Sometimes this information is referred to as "newsworthy" or matters of "public concern."

This conceptualization of public information describes a feature of the subject matter of information rather than the context within which it was disclosed. The rationale behind endowing this conceptualization of public information with exculpatory power is that in many contexts peoples' privacy interests will be overridden by benefits of a more public disclosure or society's "right to know."

For example, the disclosure tort requires a plaintiff to show that the information at issue is not a "matter of legitimate public concern" before relief can be granted.[228] The law of defamation requires a plaintiff to prove the defendants acted with "actual malice"—knowledge of falsity or reckless disregard for the truth—when the information published "includes matters of public concern."[229] In determining whether former child prodigy William James Sidis has a privacy interest in certain aspects about his current life, the Second Circuit Court of Appeals wrote that:

> Everyone will agree that at some point the public interest in obtaining information becomes dominant over the individual's desire for privacy. Warren and Brandeis were willing to lift the veil somewhat in the case of public officers. We would go further, though we are not yet prepared to say how far. At least we would permit limited scrutiny of the "private" life of any person who has achieved, or has had thrust upon him, the questionable and indefinable status of a "public figure."[230]

The court refused to grant Sidis relief based largely on the fact that his personal information was of interest to society and, thus, made him a "public" figure.

Joel Reidenberg suggested applying a "public significance filter" to questions of privacy in public in order to avoid the problems associated with focusing solely on the observability of information or acts.[231] Jonathan Mintz noted that

---

[228] Green v. Chi. Tribune Co., 675 N.E.2d 249, 255 (Ill. App. Ct. 1996) ("In our view, however, the relevant inquiry is whether *the photograph of plaintiff's dead son and her statements to him* are of legitimate public concern.").

[229] Connick v. Myers, 461 U.S. 138, 147-48 (1983) (stating that determining whether "speech addresses a matter of public concern must be determined by the content, form, and context of a given statement, as revealed by the whole record"); N.Y. Times Co. v. Sullivan, 376 U.S. 254, 281-82 (1964) ("The constitutional guarantees require, we think, a federal rule that prohibits a public official from recovering damages for a defamatory falsehood relating to his official conduct unless he proves that the statement was made with 'actual malice.'").

[230] Sidis v. F-R Pub. Corp., 113 F.2d 806, 809 (2d Cir. 1940).

[231] Reidenberg, *supra* note 22, at 155 ("The distinction means that the *nature* of the act places information into the true public sphere rather than the *observability* of the act. This distinction already has a basis in constitutional thought. In *Florida Star v. B.J.F.*, a newspaper published the name of a rape victim in violation of Florida law. The Court held that the First Amendment protected the newspaper's publication because the victim's name was obtained lawfully and because the matter (a publicized criminal proceeding) was of *public* significance.

the formidable protection afforded to publishing things of legitimate interest to society "is greatly enhanced by the relatively amorphous, and thus far-reaching, definitions of 'in the public interest,' 'news-worthy,' and 'news.'"[232] Mintz asked, "Is the term 'newsworthy' a descriptive predicate, intended to refer to the fact that there is widespread public interest? Or is it a value predicate, intended to indicate that the publication in question is a meritorious contribution and that the public's interest is praiseworthy?"[233] I do not intend to take up in this Article the question of what is newsworthy, but I reference its ambiguity to point out that, like the concept of privacy, even nuanced articulations of what is public are contested.

B. *Anything That Is "Not Private"*

Every year near the beginning of my Information Privacy Law course, before we dive into doctrine, I call on each student and ask them to define the concept of privacy to the class. As you might expect, I usually get a variety of answers, ranging from "control over information" to "secrets" to "dignity" and everything in between. Almost every year at least one student defines privacy as "everything that isn't public." I also ask the students at some point in the semester to define the concept of "public" for me. Again, I get many different answers. And nearly every year, at least one student says "everything that isn't private."

I call this the "negative" conceptualization of public. We define the concept by what it is not, referring to the notion of privacy, instead of what it is. The upside to this approach is that it simplifies the number of complex constructs at play and channels our questions straight to what constitutes privacy. The downside is that it can sometimes force us to think of privacy in terms of an overly simplistic dichotomy between public and private.

One way in which this "negative" view of public information is represented is within the construct of public and private spheres. Nissenbaum wrote "that theories of privacy should . . . recognize the systemic relationship between privacy and information that is neither intimate nor sensitive and is drawn from public spheres."[234] Under some conceptualizations, however, in public spheres our autonomy is more justly curtailed, whereas the private spheres should remain free from interference.[235] Other scholars inversely use the term "public" to

Applying a public significance filter to the transparency and publicity of personal information seems promising as a means to restore privacy in public.").

[232] Mintz, *supra* note 22, at 442.

[233] *Id.*

[234] Helen Nissenbaum, *Protecting Privacy in an Information Age: The Problem of Privacy in Public*, 17 LAW & PHIL. 559, 559 (1998).

[235] Pongrace, *supra* note 28, at 1196 ("The private sphere is that area of human activity presumptively outside the legitimate bounds of government regulation or coercion. . . . Conversely, the public sphere is that area of human activity that the government may legitimately regulate." (footnote omitted)).

define the concept of privacy. Professor Milton Konvitz referred to privacy as "a sphere of space that has not been dedicated to public use or control."[236] Harry Kalven also viewed privacy as a non-delimiting "residual" interest: "[W]hat is left after the state or society has made its demand."[237] But again, this leads us to the as yet unanswered question as to what "public" means.

Most of the sources of law I reviewed for this Article do not explicitly adopt negative conceptualizations of public information. Instead, courts, lawmakers, and regulators usually deploy the term "public" without much clarification. This substantial ambiguity is what makes reliance on public information a problem.

The negative conceptualization of public information is more often seen in discussions about the "public domain" in intellectual property regimes. Recall that in intellectual property, some conceptualizations describe the public domain as the common pool of knowledge and information not protected by intellectual property laws, though this a contested concept.[238] The idea of "public" as "negative space," or as the "body of common resources" defined by what is *not* a common resource, is popular among some. This notion treats public information as the "residual existence" or "regulatory leftovers" and operates under a sort of implied waiver theory.[239] If it is not protected by law, then it is fair game.

Using "public information" as shorthand for "that which is not protected by privacy law" might not be inherently problematic. It might actually help reduce definitional ambiguity by being deferential to other concepts, such as privacy, that should be the focus of clarification efforts. This way, courts and lawmakers can cut down on dueling ambiguity and inconsistency.

The problem with the negative conceptualization of public information comes when it is used consequentially in privacy law and policy. Used this way, the negative conceptualization deflects a substantive determination regarding the status of information by bootstrapping and perpetuates a tautology. Those who subscribe to and deploy the negative conceptualization of public information to justify surveillance and data practices are assuming the publicness of information in their argument that information is public. In other words, it makes no sense to say "this information is not private because it is public" when what is meant is "this information is not private because it is not private."

C. *Designated as Public*

The final way to conceptualize public information is an official designation or category by a relevant authority that indicates the information is for general use by anyone, or that the surveillance of certain people or acts that are exposed

[236] Milton R. Konvitz, *Privacy and the Law: A Philosophical Prelude*, 31 LAW & CONTEMP. PROBS. 272, 280 (1966).

[237] Kalven, Jr., *supra* note 29, at 327.

[238] Edward Samuels, *The Public Domain in Copyright Law*, 41 J. COPYRIGHT SOC'Y U.S.A. 137, 141 (1993).

[239] *See* Mintz, *supra* note 22, at 456-57.

to others are explicitly permitted. The most common example of something designated as public is a "public record," sometimes referred to in law as open records. These records, when released, have been designated as "public" through legislation and a deliberative process that weighed any possible exemptions. Their designation as a public record carries with it the imprimatur of government authorization as well as a signal to society that these documents are intended to be collected, used, and shared. Another example of legal regimes designating acts as public is open meetings laws, sometimes called "sunshine laws."[240] These laws prohibit denying access to the general public and are meant to encourage transparency though reporting. When meetings are subject to sunshine laws, they are sometimes said to be "public meetings."[241]

While the purpose of designating information held by the government as public is usually motivated by a desire for transparency and accountability, many other values can be served by designating information as "public." For example, "open data," meaning generally "data that can be freely used, re-used and redistributed by anyone" is also colloquially a form of designated public information.[242] The goal of open data initiatives is to increase transparency, better reproducibility, and create a quicker path to new knowledge and discovery.[243] Open data can include personal information, though it is regularly

[240] *See* Charles N. Davis, Milagros Rivera-Sanchez & Bill F. Chamberlin, *Sunshine Laws and Judicial Discretion: A Proposal for Reform of State Sunshine Law Enforcement Provisions*, 28 URB. L. 41, 41 (1996) ("Deeply imbedded in the principles of democratic government is the notion that the processes of government should be open to public scrutiny. Central to this cause are open meetings or 'sunshine' laws requiring governmental bodies to give the public access to the decision-making process in the form of public meetings."); Daxton R. "Chip" Stewart, *Let the Sunshine in, or Else: An Examination of the "Teeth" of State and Federal Open Meetings and Open Records Laws*, 15 COMM. L. & POL'Y 265, 265-66 (2010) (describing open access laws as "sunshine laws" which ensure that government meetings and records are available to public).

[241] *See* Open and Public Meetings Act, UTAH CODE ANN. § 52-4-303 (West 2006) ("A person denied any right under this chapter may commence suit in a court of competent jurisdiction to: (a) compel compliance with or enjoin violations of this chapter; or (b) determine the chapter's applicability to discussions or decisions of a public body.").

[242] *What Is Open Data?*, OPEN DATA HANDBOOK, http://opendatahandbook.org/guide/en/what-is-open-data [https://perma.cc/48ZA-YGFS] (last visited Feb. 15, 2019) (defining open data, including that it be "subject only, at most, to the requirement to attribute and sharealike [sic]"). Open data has also been defined as "information that is accessible to everyone, machine readable, offered online at zero cost, and has no limits on reuse and redistribution." Emmie Tran & Ginny Scholtes, Open Data Literature Review (2015) (unpublished symposium response), https://www.law.berkeley.edu/wp-content/uploads/2015/04/Final_OpenDataLitReview_2015-04-14_1.1.pdf [https://perma.cc/UL5X-P5SS]; *see also* BUDAPEST OPEN ACCESS INITIATIVE, http://www.budapestopenaccessinitiative.org [https://perma.cc/KMH3-ERX6].

[243] INST. OF MED., *Appendix B: Concepts and Methods for De-Identifying Clinical Trial Data*, *in* SHARING CLINICAL TRIAL DATA: MAXIMIZING BENEFITS, MINIMIZING RISK 203, 214 (2015) (emphasizing importance of de-identification).

protected through concepts like deidentification and controlled access.[244] Open data is commonly described as "public" both colloquially and officially.[245] In their document, "The 8 Principles of Open Government Data," a group of open government advocates wrote that, "[p]ublic data is data that is not subject to valid privacy, security or privilege limitations."[246] In their Open Data Policy guidelines, the Sunlight Foundation provided that, "[t]o be completely 'open,' public government information should be released completely into the worldwide public domain and clearly labeled as such."[247] It is worth noting that the Sunlight Foundation and other open data advocates also have provided guidelines to "Appropriately Safeguard Sensitive Information."[248]

The designation of information as "public" is legally significant, not just because it makes it more accessible, but also because it signals legal validation to those who wish to collect and use it. For example, the *Restatement (Second) of Torts* defers to the notion of matters of public record in determining what is private:

> [T]here is no liability for giving publicity to facts about the plaintiff's life that are matters of public record, such as the date of his birth, the fact of his marriage, his military record, the fact that he is admitted to the practice of medicine or is licensed to drive a taxicab, or the pleadings that he has filed in a lawsuit. On the other hand, if the record is one not *open* to public inspection, as in the case of income tax returns, it is not public, and there is an invasion of privacy when it is made so . . . . When these intimate details of his life are spread before the public gaze in a manner highly offensive to the ordinary reasonable man, there is an actionable invasion of his privacy, unless the matter is one of legitimate public interest.[249]

---

[244] *See* Ira S. Rubinstein & Woodrow Hartzog, *Anonymization and Risk*, 91 WASH. L. REV. 703, 720 (2016) (using genetic research as example of importance of controlled access).

[245] *See, e.g.*, Marin Kress, *By the Numbers: Port Statistics for Some of the Largest U.S. Ports*, DATA.GOV (Mar. 1, 2017), https://www.data.gov/maritime/p24529331/ [https://perma.cc/QMZ4-M42M] ("The 2016 Port Performance report used multiple sources, including *public datasets* featured on Data.Gov." (emphasis added)).

[246] *The Annotated 8 Principles of Open Government Data*, DATA.GOV, https://opengovdata.org [https://perma.cc/W7VC-VWSY] (last visited Feb. 15, 2019) (including complete, primary, timely, accessible, machine processable, non-discriminatory, non-proprietary, and license-free).

[247] *Open Data Policy Guidelines*, SUNLIGHT FOUNDATION, https://sunlightfoundation.com/opendataguidelines [https://perma.cc/L67D-HNZN] (last visited Feb. 15, 2019).

[248] *Id.* (noting that internal data policy can serve to supplement legislative protection).

[249] RESTATEMENT (SECOND) OF TORTS § 652D (AM. LAW INST. 1977) (emphasis added) ("Similarly, there is no liability for giving further publicity to what the plaintiff himself leaves open to the public eye . . . . Every individual has some phases of his life and his activities and some facts about himself that he does not expose to the public eye, but keeps entirely to himself or at most reveals only to his family or to close friends.").

It is not clear if "matter of public record" here means information that is available, widely known, or designated "public" by the government. However, given the items listed by the *Restatement*, it would seem to be records designated as "public" and made available by the government.

Courts often give deference to the fact that public records are "lawfully obtained" when determining what information is private and what information is in the "public domain" (and thus not private).[250] In a series of privacy tort cases that denied the plaintiff's recovery, the defendants divulged information that they lawfully obtained from what the Court referred to as the "public domain."[251] Mintz wrote:

> The public domain component of each of the Court's disclosure decisions was clearly of crucial analytical importance. In *Cox Broadcasting Corp. v. Cohn*, the Court stated repeatedly that the information was obtained from courthouse records that were open to public inspection, and that the information had been placed "in the public domain on official court records." Moreover, the *Cox Broadcasting* Court noted that because the disclosed information came from "public records generally available to the media," affirming liability against the defendant would then give rise to "timidity and self-censorship."[252]

The Supreme Court in *Smith v. Daily Mail Publishing Co.*[253] also referenced notions of information that was "lawfully obtained," "publicly revealed," and in the "public domain" in stating that those concepts "suggest strongly" that the Constitution prohibit punishing speakers for publishing matters of public significance that were obtained lawfully.[254] And in *Florida Star v. B.J.F.*,[255] the Court looked to whether information was "lawfully obtained" because it was "furnished by the government" in determining contested disclosures involving information in the "public domain" and, thus, could not be lawfully constrained.[256]

The justification behind validating information that has been designated as public is based upon more than just a description of the information's context or failing to find a privacy interest. It is value-driven. Many reasons can justify

---

[250] *See* Mintz, *supra* note 22, at 456-57 (citation omitted).

[251] *See* Fla. Star v. B.J.F., 491 U.S. 524, 536 (1989) (obtaining personal information of sexual assault victim); Smith v. Daily Mail Publ'g Co., 443 U.S. 97, 99 (1979) (monitoring police band radio frequency to obtain and publish defendant's personal information); Cox Broad. Corp. v. Cohn, 420 U.S. 469, 495 (1975) (broadcasting name of rape victim).

[252] *See* Mintz, *supra* note 22, at 456 (quoting *Cox Broad. Corp.*, 420 U.S. at 495-96).

[253] 443 U.S. 97 (1979).

[254] *Id.* at 103; *see* Mintz, *supra* note 22, at 456.

[255] 491 U.S. 524 (1989).

[256] *Id.* at 535 ("As *Daily Mail* observed in its summary of *Oklahoma Publishing*, 'once the truthful information was publicly revealed or in the public domain the court could not constitutionally restrain its dissemination.'" (quoting *Daily Mail Publishing Co.*, 443 U.S. at 103)).

designating information as public, including government accountability, research, industry and market support, facilitation of government services, civic participation, and much more. Privacy is part of the calculus in determining what is to be collected, sorted, and released. But this notion of public includes goals and procedures that are about more than "personal information."

*****

The concept of public information is remarkably ambiguous. In this Part, I have attempted to add some nuance to it and impose some organization on it. The law and literature reveal three general ways to define what is public: (1) description, (2) "not private," and (3) designation. How the concept is defined will determine its power and legitimacy in privacy law and policy. In the next part, I make an appeal for clarity.

III. WHAT IS "PUBLIC" MUST BE CLARIFIED

In this Article, I hope to make one point very clear: we should be skeptical and deliberate when deploying the concept of public information in a legally significant way because it can be conceptualized several different and value-laden ways. It is a mistake to validate the "no privacy in public" argument without being clear about what public even means. In this Part, I propose a path to precision.

First, I argue that regardless of which conceptualization is adopted, privacy law and policy should recognize labeling information as public is a value-laden exercise of power. The normative choices made in law are most evident in the "designation" conceptualization of public information. For example, sometimes privacy concerns surrounding information in public records are overridden because releasing information is in the "public interest." And of course the "not private" conceptualization also compels us to ask the normatively fraught question of "what is privacy?" However, even descriptive accounts of public information are value judgments. The problem with the descriptive conceptualization of "privacy" is that these values that shape the described boundaries are not always apparent because the descriptive accounts are often presented as neutral observations, as though the common boundaries of what is public were set and ascertainable in the same way as the metes and bounds of property lines.

Next, I propose that to the extent descriptive factors are an important part of determining what constitutes public information, some of the common frameworks are out of whack. In particular, notions of hypothetical accessibility and exposure regularly fail to properly account for what shapes peoples' perceptions and behavior. I argue the concepts of obscurity and trust should be better considered in the descriptive calculus about what constitutes public information. Obscurity and trust play a key role in shaping people's decisions about when, where, how, and with whom to share information or interact with others. To ignore these factors renders notions that public information is based

on hypothetical accessibility harsh and repressive. In theory, virtually everything we do is accessible to someone, somewhere. And this mistake is at the heart of our approach to many modern privacy quandaries.

A. *Public Is a Value Judgment*

In this Article I have catalogued the various ways in which courts and lawmakers treat the concept of public as though it is an objective, pre-existing state that need only be ascertained by looking to degrees of accessibility and exposure, which then determine people's privacy interests in their information and acts. But this is a misguided approach to public information. To say something is "public" is to make a value-laden conclusion about what information should be protected and what kinds of surveillance and data practices should be permissible. It is an exercise of power.[257]

The semantic ambiguity of public information means that implementation of the concept requires many different assumptions about the resources, motivations, abilities, and pre-existing knowledge of people who make up "the public." It also requires assumptions about norms, architectural restraints, traffic density and timing, and the relative visibility, audibility, and comprehensibility of the acts to be surveilled or the data to be collected. By the time all of these assumptions are made, the idea of public becomes a construct further removed from empirical observation with the conclusion of what is "public" determined by the thresholds and boundaries set by these assumptions.

For example, those seeking to justify broad and pervasive surveillance would be best off conceptualizing public information as all that is "freely accessible." This category is the most inclusive because it allows for the most conjecture about who *could* see or access information, rather than who actually did. Conjecture about exposure is difficult to rebut. For example, anyone *could* have seen you quickly fix a wedgie while you were outside or could briefly walk by your hotel room window while you were in your underwear, but the odds are low. Meanwhile the designated and "widely known" conceptualizations of public information are narrower. A comparatively miniscule amount of information in the world is ever designated as public information. Public records are only a small part of the world's data ecosystem. And hardly anyone except you actually knows your exact daily routine and everything you share online.[258]

---

[257] *See* Cohen, *supra* note 35, at 213-14 ("The process of constructing a public domain begins with an act of imagination that doubles as an assertion of power. An identifiable subject matter—a part of the natural world or an artifact of human activity—is reconceived as a resource that is unowned but potentially appropriable, either as an asset in itself or as an input into profit-making activity. The biopolitical public domain is a construct tailored to the political economy of informational capitalism. It constitutes the field of opportunity for a particular set of information-based extractive endeavors.").

[258] Except, perhaps, your internet service provider ("ISP"). But that is a different fight altogether.

Those who set the framework to determine what is public can predetermine the winner before the questions are even asked.

The United Kingdom's Information Commissioner's Office's ("ICO") approach to determine what falls into the public domain is an example of how to treat the concept of public information as a prescriptive, not descriptive concept. The ICO has a relatively nuanced approach to what constitutes falling within the public domain. Critically, it determined that "[e]ven if the information itself is already in the public domain, this is not decisive and is not an automatic argument either for or against disclosure."[259] Rather, several different considerations must be weighed before the decision to make information freely available is made.

Likewise, the jurisprudence of the privacy exemption built into the Federal Freedom of Information Act ("FOIA") and similar state laws has reflected the idea that:

> An individual's interest in controlling the dissemination of information regarding personal matters, however, does not dissolve simply because that information may be available to the public in some form or from other sources. In other words, the fact that otherwise private information at one time or in same way may have been placed in the public domain does not mean that a person irretrievably loses one's privacy interest in that information or has no interest in limiting the disclosure or dissemination of the information. In particular, even if information was at some time or place publicly available, a privacy expectation may exist if the information is now hard to obtain and, for a practical matter, now obscure.[260]

This recognition of labeling information public as a value judgment should be better integrated into privacy law and policy.

The benefit of explicitly treating "public" as a prescriptive, value-laden concept is that it helps facilitate the debate when values such as free speech, privacy, and security conflict. There are often good reasons to favor free speech over privacy in certain contexts, but by cloaking the concept of public information entirely in descriptive terms, we obscure the value choices at stake and disadvantage privacy by creating presumptions of the public nature of information using questionable assumptions about behavioral norms and societal expectations.

B. *Towards a More Accurate Notion of Public Information*

While determining the public nature of information is not exclusively a descriptive question, descriptive factors such as the degree of exposure and internalized knowledge are relevant, even in some regimes that designate

[259] INFO. COMM'R'S OFFICE, INFORMATION IN THE PUBLIC DOMAIN 11 (2013), https://ico.org.uk/media/for-organisations/documents/1204/information-in-the-public-domain-foi-eir-guidance.pdf [https://perma.cc/J3HW-ZHRV].

[260] 37A AM. JUR. 2D FREEDOM OF INFORMATION ACT § 239 (1994).

information as public. But, as Julie Cohen has written, "interpreting self-exposure either as a blanket waiver of privacy or as an exercise in personal empowerment would be far too simple."[261] The problem is that too often the framework for assessing the degree of exposure or accessibility gives short shrift to two of the most important factors that shape peoples' behavior and perceptions of risk in any given environment—the obscurity of people and data and the existence of relationships of trust. People feel relatively safe when their acts and data exist in zones of obscurity and are disclosed within relationships of trust. If disclosing information in "public" is going to act as a waiver of sorts to justify surveillance and data practices, then the concept should at least rest on a more accurate assessment of social behavior and risk.

1. Zones of Obscurity

Obscurity as a privacy value is the notion that when our activities or information is unlikely to be found, seen, or remembered, it is, to some degree, safe. People calculate risk every day based upon how obscure they are or are likely to be. For example, you probably feel comfortable discussing relatively sensitive topics (or perhaps just gossiping) over dinner in a public restaurant because the likelihood of that disclosure being more publicly disseminated or coming back to harm you is pretty low. You are in a room full of strangers. They are probably not eavesdropping.

In work with Proefssor Evan Selinger and Fred Stutzman, I have explored the concept of obscurity as an essential component of modern notions of privacy.[262]

[261] Cohen, *supra* note 165, at 198.

[262] *See* Woodrow Hartzog & Evan Selinger, *Surveillance as Loss of Obscurity*, 72 WASH. & LEE L. REV. 1343, 1356 (2015) (explaining etymology of obscurity); Woodrow Hartzog & Frederic Stutzman, *The Case for Online Obscurity*, 101 CAL. L. REV. 1, 24 (2013) [hereinafter Hartzog & Stutzman, *The Case for Online Obscurity*] (attacking idea that information is either disseminated globally or completely secret); Woodrow Hartzog & Frederic Stutzman, *Obscurity by Design*, 88 WASH. L. REV. 385, 387 (2013) (noting that modern understanding of privacy has created list of unaddressed problems); Evan Selinger & Woodrow Hartzog, *Obscurity and Privacy*, *in* SPACES FOR THE FUTURE: A COMPANION TO PHILOSOPHY OF TECHNOLOGY 119, 119 (Joseph Pitt & Ashley Shew eds., 2017) ("Obscurity is the idea that information is safe—at least to some degree—when it is hard to obtain or understand."); Woodrow Hartzog & Evan Selinger, *Obscurity: A Better Way to Think About Your Data Than "Privacy"*, ATLANTIC (Jan. 17, 2013), http://www.theatlantic.com/technology/archive/2013/01/obscurity-a-better-way-to-think-about-your-data-than-privacy/267283/ (explaining that absence of privacy does not always result in lack of safety); 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 (describing obscurity as important concept for protection of personal privacy); Evan Selinger & Woodrow Hartzog, Opinion, *Google Can't Forget You, But It Should Make You Hard to Find*, WIRED (May 20, 2014, 3:33 PM), http://www.wired.com/2014/05/google-cant-forget-you-but-it-should-make-you-hard-to-find/ ("This debate is not and should not be about forgetting or disappearing in the traditional sense. Instead, let's

Every day we make decisions about where we go, what we do, and what we share based upon how obscure we think we are. Most of our information online is obscure as well. For example, just because information is hypothetically available does not mean most (or even a few) people have the knowledge and ability to access information. Without the right search terms, URL, access credentials, or pre-existing knowledge to make sense of data, information will remain obscure. We are all at least subconsciously aware of this reality and adjust our risk calculus accordingly. I have argued that obscurity is heavily relied upon as a form of privacy in the modern age.[263] Yet these societal expectations of obscurity are regularly overlooked when public information is conceived of as freely accessible and endowed with the power to defeat privacy claims.[264]

Some pockets of privacy law recognize the importance of obscurity with respect to public information better than others. Recall the Supreme Court's *Reporters Committee* that recognized a privacy interest in the "practical obscurity" of disaggregated public records. This privacy interest is grounded in the notion of how transaction costs can make certain bits of information hard or unlikely to be found, and that these costs can shift over time. The Court wrote that "the extent of the protection accorded a privacy right at common law rested in part on the degree of dissemination of the allegedly private fact and the extent to which the passage of time rendered it private."[265] The passage of time makes information harder to recall because people forget things, records get lost, databases get deleted, and links rot. Information has a natural way of becoming obscure. Even at the micro-level, social applications like Snapchat that build in a sort of ephemerality are seeking to encourage disclosure by manufacturing some sense of obscurity for users. Assuming they are not saved by a screenshot, "Snap" photos become practically obscure after a few seconds because they are only retrievable through a considerable expense of resources.

Another example of attempts to integrate obscurity into public information doctrine comes from the United Kingdom's ICO's guidance on public records

recognize that the talk about forgetting and disappearing is really concern about the concept of obscurity in the protection of our personal information.").

[263] *See* sources cited *supra* note 262; *see also* Blitz, *supra* note 159, at 27-28 (proposing technology-based test for limiting public surveillance that is precisely targeted at role of transaction costs in making surveillance easier or more difficult); Solove, *supra* note 72, at 1178 ("Privacy involves an expectation of a certain degree of accessibility of information. Under this alternative view, privacy entails control over and limitations on certain uses of information, even if the information is not concealed. Privacy can be violated by altering levels of accessibility, by taking obscure facts and making them widely accessible."); Harry Surden, *Structural Rights in Privacy*, 60 SMU L. REV. 1605, 1607 (2007) ("In the privacy context, society implicitly relies upon non-legal regulators to prevent a large number of unwanted behaviors.").

[264] Hartzog & Stutzman, *The Case for Online Obscurity*, *supra* note 262, at 24.

[265] U.S. DOJ v. Reporters Comm. for Freedom of the Press, 489 U.S. 749, 763 (1989).

regarding what information is in the "public domain."[266] The ICO has determined that "[i]nformation is only in the public domain if it is *realistically* accessible to a member of the general public at the time of the request. It must be available *in practice*, not just in theory."[267] The ICO goes on to provide nuance, stating that:

> [I]nformation will not be in the public domain if it would require unrealistic persistence or specialised knowledge to find it, even if it is theoretically available somewhere in a library or on the internet. In practice a normal member of the public would still not be able to find that information.[268]

The ICO defined a member of the general public as "a hypothetical average member of the general public who is interested enough to conduct some searches for the information, but does not possess any specialised knowledge or research skills."[269]

This conceptualization can be contrasted to cases in the United States that assume merely because a website is hypothetically available to anyone who just happened to have knowledge of a URL or the right search terms (no matter how obscure), it is public information.[270] The ICO stated that:

> In particular, information is not necessarily in the public domain just because it is known to the requester. The question is still whether a hypothetical interested member of the public could access the information . . . . And on the other hand, information may be in the public domain even if the requester could not access it because of their personal circumstances (for example, because they have no access to the internet). Availability to the individual requester is irrelevant. The question is whether it is available to a hypothetical member of the public. This question of public availability should not be confused with reasonable accessibility to the individual applicant.[271]

---

[266] *See generally* INFO. COMM'R'S OFFICE, *supra* note 259 (providing guidelines for what falls within public domain).

[267] *Id.* at 2 (emphasis added).

[268] *Id.* at 5-6.

[269] *Id.* at 6 (citations omitted).

[270] *See* Hartzog & Stutzman, *The Case for Online Obscurity*, *supra* note 262, at 24 (citing Boring v. Google Inc., 362 F. App'x 273 (3d Cir. 2010); then citing Guest v. Leis, 255 F.3d 325, 333 (6th Cir. 2001); then citing Sandler v. Calcagni, 565 F. Supp. 2d 184 (D. Me. 2008); then citing United States v. D'Andrea, 497 F. Supp. 2d 117 (D. Mass. 2007); then citing Four Navy Seals v. Associated Press, 413 F. Supp. 2d 1136 (S.D. Cal. 2005); then citing United States v. Gines-Perez, 214 F. Supp. 2d 205 (D.P.R. 2002); then citing Moreno v. Hanford Sentinel, Inc., 91 Cal. Rptr. 3d 858, 862-63 (Ct. App. 2009); then citing Yath v. Fairview Clinics, N.P., 767 N.W.2d 34 (Minn. Ct. App. 2009); then citing State v. Birchfield, No. 04-08-00132, 2007 WL 1437235 (N.J. Super. Ct. App. Div. May 17, 2007)).

[271] INFO. COMM'R'S OFFICE, *supra* note 259, at 7-8.

The transaction costs for accessing information also change over time. Information thus becomes more or less obscure, which alters people's risk calculus and privacy expectations. The impermanence of exposure should be better reflected in U.S. privacy law. For example, the ICO said in regards to whether something is in the "public domain," information must be "available at the time of the request."[272] This conceptualization gets closer to capturing the role of transaction costs in finding and understanding information and the natural obscurity produced by mere passage of time.

In summary, the question of what is public is often just the threshold line that is drawn somewhere on the spectrum of things that range from completely obscure to totally obvious or known. People value their obscurity and build their disclosures and acts in reliance upon it. The calculus for what makes things obscure is complex and includes many different factors like searchability; permanence; comprehensibility; identifiability; and the resources, motivation, and pre-existing knowledge of those who seek to surveil or make use of data. These factors should be better valued when formulating accounts of public information.

2. Relationships of Trust

The other most important factor relevant to how people perceive risk, choose to expose themselves, and share information that too often gets glossed over in descriptive accounts of public information is the role of relationships of trust. In previous work with Professor Neil Richards, I argued that trust—the willingness to accept vulnerability to the actions of others—is necessary for a safe and sustainable digital world.[273] We wrote, "In the privacy context, trust allows us to develop long-term, sustainable information relationships by sharing meaningful but often sensitive information and having sincere exchanges with the confidence that what we share will be used for our benefit and not come back to haunt or harm us."[274] Professor Ari Ezra Waldman has conceptualized privacy itself as "a behavioral exchange of trust and discretion."[275] If we cannot trust others with our personal information, society will suffer.

[272] *Id.* at 8-9 ("Even if information has entered the public domain some time before the date of the request, this does not mean it remains there indefinitely. Even if the information was at one time considered a matter of public record (eg by being revealed in open court) or was otherwise previously published or disseminated (eg in response to an earlier FOI request), this does not mean it is still available in practice at the time of the request.").

[273] *See* Neil Richards & Woodrow Hartzog, *Taking Trust Seriously in Privacy Law*, 19 STAN. TECH. L. REV. 431, 435 (2016) (arguing that lack of trust creates pessimism regarding privacy law).

[274] Neil Richards & Woodrow Hartzog, *Privacy's Trust Gap*, 126 YALE L.J. 1180, 1213 (2017).

[275] Ari Ezra Waldman, *Privacy As Trust: Sharing Personal Information in a Networked World*, 69 U. MIAMI L. REV. 559, 630 (2015).

Trust is everywhere. Our modern networked world is mediated by what Richards and I referred to as "information relationships," in which "professionals, private institutions, or the government hold information about us as part of providing a service."[276] These relationships surround us—"when we share sensitive personal information with Internet service providers (ISPs), doctors, banks, search engines, credit card companies, and countless other information recipients and intermediaries."[277] Even traditional merchants that people interacted anonymously with like grocery stores have gotten into the game:

> Merchants use data to predict what shoppers will do. Companies give away products and services "for free" just to get the information that comes with it. Data brokers amass vast troves of data to enable their clients to profile, segment, and influence people as consumers or as voters. The stampede for big data and the development of the "Internet of Things" are only accelerating these developments.[278]

This is to say nothing of our interpersonal relationships, where we gossip, share secrets, and expose our feelings and weaknesses. Trust is not just a fundamental component of privacy. It is the glue that holds society together.

But relationships of trust are often seemingly glossed over in determining what information is public. Concepts like the "third party doctrine" treat disclosures to anyone, no matter how trusted, as a waiver of privacy rights.[279] The privacy torts are maddeningly inconsistent in their recognition of trusted confidants.[280] Privacy law, it seems, is often content to treat disclosures to

---

[276] Richards & Hartzog, *supra* note 273, at 433.

[277] *Id.* at 433-34.

[278] *Id.*

[279] *See, e.g.*, Jack M. Balkin, *Information Fiduciaries and the First Amendment*, 49 U.C. DAVIS L. REV. 1183, 1230 (2016) (arguing against third party doctrine's assumption that when people disclose information to third party, disclosers have "no reasonable expectation of privacy in the information" and proposing, instead, that many third parties "owe us fiduciary duties or duties of confidentiality"); Kiel Brennan-Marquez, *Fourth Amendment Fiduciaries*, 84 FORDHAM L. REV. 611, 611, 616 (2015) (arguing that third party doctrine should be limited where person shares information with "information fiduciary").

[280] *See* Fisher v. Ohio Dep't of Rehab. & Corr., 578 N.E.2d 901, 903 (Ohio Ct. Cl. 1988) ("The court agrees with the defendant that the report merely recounts a conversation which the plaintiff *publicly* and openly conducted with her fellow employees. The plaintiff's discussion of her personal experiences were freely offered to the *persons around her* without concern of the impact it might have on her character." (emphasis added)); Strahilevitz, *supra* note 87, at 920-21 ("Despite the centrality of this issue, the American courts lack a coherent, consistent methodology for determining whether an individual has a reasonable expectation of privacy in a particular fact that has been shared with one or more persons.").

anyone outside of narrowly prescribed, formalized confidential relationships as "public."[281] This is a problem.

Modern accounts of public information should better consider relationships of trust in their decision-making framework. If obscurity is concerned with who *might* see us or find our information, trust is the relevant factor for evaluating whether the *actual* recipients of information render certain disclosures public. These recipients need not be full-fledged "confidants" in the formal sense of the word. People trust others to be discrete, loyal, honest, and protective all the time without demanding a formal obligation of confidentiality. They adjust their risk calculus on this trust and the likelihood that information will not travel too far or be used against them.[282] If we want this kind of trust to continue (and we should) our law and policy should accommodate it when labeling and evaluating what is public.

We can see bits of respect for trust at the margins of privacy law and policy, particularly the law of public records. Formal promises of confidentiality are "generally given weight with regard to an individual's expectation of privacy" and the privacy exception of FOIA.[283] The ICO holds that "[i]nformation disclosed only to a limited audience will not generally be in the public domain, as it is unlikely to be available to a member of the general public."[284] This is an implicit recognition that limited disclosures generally carry with them expectations of discretion and loyalty—two hallmarks of trust in relationships.

One way to better account for trust in the law and policy of public information would be to seek to develop and identify common indicators of trust. This might include looking to such factors as custom, the kind of relationships between the discloser and the recipients, the purpose of a disclosure, whether a disclosure was solicited, the relative sophistication and power between the parties, and any communication through words or design that trust would be kept.[285] Helen Nissenbaum has proposed that conditions of trust include recipient's history and

---

[281] *See* Woodrow Hartzog, *Reviving Implied Confidentiality*, 89 IND. L.J. 763, 764 (2014) ("At best, the concept of implied confidentiality plays a negligible role in the developing doctrine surrounding modern privacy disputes.").

[282] Strahilevitz, *supra* note 87, at 930 (discussing how trust builds intimacy and willingness to reveal certain information).

[283] 37A AM. JUR. 2D FREEDOM OF INFORMATION ACT § 239 (1994) ("[O]ther things being equal, the release of personal information provided under a pledge of confidentiality involves a greater invasion of privacy than the release of information provided without such a pledge, for the purpose of applying the personal privacy exemption." (citing U.S. Dep't of State v. Ray, 502 U.S. 164 (1991); then citing District of Columbia v. Fraternal Order of Police, Metro. Police Dep't Labor Comm., 75 A.3d 259 (D.C. 2013); then citing Wash. Post Co. v. U.S. Dep't. of Health and Human Servs., 690 F.2d 252 (D.C. Cir. 1982); then citing Ray v. U.S. DOJ, 908 F.2d 1549 (11th Cir. 1990), *judgment rev'd on other grounds*, 502 U.S. 164 (1991))).

[284] INFO. COMM'R'S OFFICE, *supra* note 259, at 6.

[285] For a more complete list of the factors courts look at in determining whether a trust in the form of implied confidences exists, see Hartzog, *supra* note 281, at 774-800.

reputation, inferences about the recipient's trustworthiness based on personal characteristics, mutuality and reciprocity within relationships, reliance on the recipient filling a role (such as doctor, merchant, ISP), and other contextual factors.[286] The literature and empirical evidence for what might indicate a relationship of trust is vast and should not be ignored in privacy law.[287]

CONCLUSION

The debate over privacy in public information has tied us into knots. Recognizing restrictions on public information conflicts with many traditional notions of privacy as secrecy. Yet abandoning privacy in public can feel counterintuitive, unfulfilling, and dangerous. To untie the knot, we must change the terms of the debate.

The "no privacy in public" argument has, thus far, put the cart before the horse. Before lawmakers and society can answer the question of whether privacy can exist in public, we must first understand what the concept of "public" means. As I have demonstrated in this Article, "public" can be conceptualized several different ways, from descriptive to designated. These conceptualizations are at best under-theorized and at worst tautological. This means that the term must be given a more articulated meaning to be useful in law and policy.

---

[286] Helen Nissenbaum, *Securing Trust Online: Wisdom or Oxymoron?*, 81 B.U. L. REV. 635, 643 (2001) (describing trust as "systematically responsive to variety of factors" and exploring link between trust and "variety of phenomena that function systematically as its cues, clues, or triggers").

[287] Other scholars have also proposed accommodating interpersonal relationships in the doctrine of public information. For example, Joel Reidenberg argued that in determining whether a privacy interest in public should be recognized, courts and lawmakers should look to whether an act or disclosure was "governance-related" or "non-governance-related"—what he called a "private-regarding act." Reidenberg, *supra* note 22, at 155-56.

The *Katz* decision provides a useful starting point to identify "private"-regarding acts. *See generally* Katz v. United States, 389 U.S. 347 (1967). Even though the phone call in that case took place in a publicly observable place on a street corner, one could hardly argue that the action of a person making a call in a phone booth is one of "public significance" or directed toward the public. The activity in *Katz* would be classified as private, and the outcome of the case would be the same. Similarly, the New York state prescription drug database that was addressed in *Whalen v. Roe* could not have a privacy right under the traditional "reasonable expectation of privacy" standard because the doctors' prescription records were always disclosed to third parties, the pharmacies. *See generally* Whalen v. Roe, 429 U.S. 589 (1977). The doctors' prescription records, though, are not of public significance. Rather, the medical interaction was a private interaction among the patient, doctor, and pharmacist. As such, Whalen would likely have a different result.

Professor Lior Strahilevitz has argued that courts and lawmakers should look to social network theory and research to gain some wisdom on the question of what extent of dissemination the person disclosing information "should have expected to follow his disclosure of that information to others." *See* Strahilevitz, *supra* note 87, at 921.

Most importantly, law and society must recognize that to label something as "public" is both consequential and value-laden. We must reject a neutral, empirical notion of "public" that is separate from legal and social construction. There is no such thing. How we define public information sets the rules for surveillance and data practices, so we should proceed intentionally and with caution. We should be more critical of claims like "data is public" to justify surveillance and data practices. To move forward, we should focus on the values we want to serve, the relationships and outcomes we want to foster, and the problems we want to avoid.