10-1-2014

Privacy in Public

Joel R. Reidenberg

Privacy in Public

JOEL R. REIDENBERG*

As government and private companies rapidly expand the infrastructure of surveillance from cameras on every street corner to facial recognition for photographs on social media sites, privacy doctrines built on seclusion are at odds with technological advances. This essay addresses a key conceptual problem in U.S. privacy law identified by Justice Sotomayor in United States v. Jones *and by Justice Scalia in* Kyllo v. United States*; namely that technological capabilities undermine the meaning of the third-party doctrine and the Fourth Amendment's 'reasonable expectation of privacy' standard. The essay argues that the conceptual problem derives from the evolution of three stages of development in the public nature of personal information, culminating in the ubiquitous transparency of citizens. This ubiquitous transparency destroys any "reasonable expectation of privacy." The essay then argues that transparency without privacy protection challenges the democratic values of public safety and fair governance. To restore the balance and relocate privacy away from the no longer workable "reasonable expectation" standard, the essay argues for a new normative approach to privacy that would protect observable activity where such activity is not "governance-related," but rather "private-regarding." The essay concludes by showing that this distinction is consistent with the First Amendment and draws on established doctrines in tort law and First Amendment jurisprudence.*

* Stanley D. and Nikki Waxberg Chair, Fordham University; Inaugural Microsoft Visiting Professor of Information Technology Policy, Princeton University (2013–14). This paper is based on the author's CUNY-Lehman College Annual Constitution Day Lecture and subsequent talk at the Yale Law School as part of the ISP-Knight Law and Media Series. Many thanks to Ira Bloom and his colleagues at Lehman College, Jordan Kovnot, Cameron Russell, the Yale Colloquium participants for their thoughtful comments on the lecture, and to Franziska Boehm, Angus Johnson, Michael Froomkin, Paul Ohm, Neil Richards, Woody Hartzog, and the participants at the Berkeley/GW Privacy Law Scholars Conference and the Clare College, Cambridge International Privacy Law Workshop for their comments on an earlier draft. Thanks too to Adam Elewa for his able research assistance.

I. INTRODUCTION

Data gathering drones at 17,500 feet,[1] cell phone-based GPS trackers,[2] wide distribution of facial recognition software,[3] always-connected Google Glass,[4] and social network tools all demonstrate extraordinary technical capabilities and collectively reflect that wide-scale deployment of information technology creates a very transparent world. In this technologically mediated world, privacy law and society are in a state of confusion about the appropriate treatment of publicly available personal information. More than fifteen years ago, Helen Nissenbaum wrote of 'privacy in public' and argued "an adequate account of privacy should neither neglect the nonintimate realm nor explicitly exclude it from consideration."[5] Her critique of the binary distinction between the public and private realms is all the more relevant today in the face of now ubiquitous surveillance and identifying technologies.

The transparency of personal information that is enabled by sophisticated online technologies undermines the meaning and value of longstanding American constitutional doctrines for privacy. In particular, the Fourth Amendment's "reasonable expectation of privacy" standard and corresponding third-party doctrine seem anachronistic to serve their purpose of distinguishing the borders of privacy protection.

This essay looks at the state of confusion over privacy in public. In a world of 24/7 data tracking, warehousing, and mining, technology has transformed obscurity, accessibility, and transparency of personal information in ways that subvert the utility of the "reasonable expectation of privacy" constitutional standard. This essay will first map out the key constitutional doctrines that drive privacy law in the United States and

1. *Rise of the Drones* (PBS television broadcast Jan. 23, 2013), *available at* http://www.pbs.org/wgbh/nova/military/rise-of-the-drones.html.

2. Doug Adomatis, *Using GPS for Tracking People*, TRAVEL BY GPS, http://travelbygps.com/articles/tracking.php (last visited Aug. 27, 2014) (listing and describing different services).

3. Nicole Lee, *First Taste of iLife '09: iPhoto's Face Recognition*, CNET (Jan. 30, 2009, 3:43 PM), http://news.cnet.com/8301-17938_105-10153818-1.html (millions of Facebook members also use the "tag" feature to identify people in photographs that in turn enables Facebook to automatically match those individuals in other photographs).

4. *Glass*, GOOGLE, http://www.google.com/glass/ (last visited Aug. 27, 2014).

5. Helen Nissenbaum, *Toward an Approach to Privacy in Public: Challenges of Information Technology*, 7 ETHICS & BEHAV. 207, 208 (1997).

will show that the transformation of information flows through three stages of development, which fundamentally undermines the concept of a "reasonable expectation of privacy." Information that was once private through obscurity now becomes technologically accessible. Information that was once merely accessible now becomes transparent and receives wide publicity. These parameter changes no longer fit within traditional court jurisprudence on privacy. The essay then argues that constitutional democracy depends on spheres of privacy in public to preserve public safety and fair governance. To create those spheres of privacy in public, the essay looks to a possible new demarcation line and proposes that privacy protection be framed in terms of 'governance-related' and 'non-governance-related' acts.

II. The Basic Constitutional Standards for Privacy and Technology

The First and Fourth Amendments are the most significant constitutional drivers in U.S. privacy law.[6] In broad terms, the First Amendment protects against government interference in citizens' rights to access and convey information.[7] More directly, the Fourth Amendment protects citizens' reasonable expectations of privacy against warrantless searches and seizures.[8] Of lesser magnitude for purposes of privacy, the Due Process Clause of the Fourteenth Amendment also intersects with privacy and has been construed to protect a political association from having to disclose its membership information.[9]

Fourth Amendment jurisprudence created the concept of a "reasonable expectation of privacy" that permeates the rhetoric of privacy even in areas outside of constitutional law.[10] The concept originates with the Supreme Court's decision in *Katz v. United States*.[11] Up until this decision, search and seizure law only protected individuals from the government breaking down their doors without a search warrant.[12] In the *Katz* case, however, the police, without a warrant, eavesdropped on a suspect

6. *See, e.g.*, Paul M. Schwartz & Joel R. Reidenberg, Data Privacy Law 44–50, 60–73 (1996).

7. U.S. Const. amend. I; *see also* Sorell v. IMS Health Inc., 131 S. Ct. 2653, 2667 (2011).

8. U.S. Const. amend. IV; *see also* Katz v. United States, 389 U.S. 347, 359 (1967).

9. U.S. Const. amend. XIV; *see also* NAACP v. Alabama *ex rel.* Patterson, 357 U.S. 449, 460–63 (1958).

10. *See, e.g.*, President's Council of Advisors on Science & Technology, Big Data and Privacy: A Technological Perspective 8 (2014), *available at* http://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf (referring to the perception of the continuous tracking of individuals for location based services as "a potential affront to a widely accepted 'reasonable expectation of privacy' ").

11. *Katz*, 389 U.S. 347.

12. *Id.* at 352.

who was speaking on a telephone inside a glass phone booth on a public street corner.[13] Even though the suspect's activities were in a public space and were completely visible, the Court decided that the Fourth Amendment "protect[ed] people, not places."[14] Justice Harlan articulated the now famous formulation of a "twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'"[15]

Katz was a new interpretation of the Fourth Amendment that moved away from defining privacy in terms of physical trespass to framing privacy in terms of expectations.[16] Following the *Katz* interpretation of privacy, the Fourth Amendment extended beyond physical boundaries setting the stage for much of the current instability concerning the scope of privacy for actions that occur in public.

Under *Katz* and its progeny, in order for there to be "privacy," an individual must have an expectation of privacy that society will recognize as legitimate.[17] During the two decades following the *Katz* decision, the Court tried to figure out how the accessibility of information in public places related to the expectation of privacy. The Court's inquiry into whether individuals have privacy in public gave rise to the "third-party" and "plain-view" doctrines. The jurisprudence started down this path in *United States v. Miller* when the Court ruled that the drawer of a check had no privacy interest in the transaction information contained on the check because the check was disclosed to many third parties through the banking system.[18] A few years later, the Supreme Court likewise ruled that individuals had no reasonable expectation of privacy in the phone numbers they dialed, as these numbers were necessarily disclosed to the phone company so that the call could be routed.[19] In a similar vein, the Supreme Court held in *California v. Ciraolo* that the observation of a marijuana field from a low flying airplane did not require a warrant.[20] The field, though on private property shielded from the public street, was considered to be in "plain view" or, in other words, publicly avail-

13. *Id.*

14. *Id.* at 351.

15. *Id.* at 361 (Harlan, J., concurring).

16. *Id.* at 353.

17. *See, e.g.*, Florida v. Jardines, 133 S. Ct. 1409, 1414 (2013); Illinois v. Caballes, 543 U.S. 405, 409–10 (2005); California v. Ciraolo, 476 U.S. 207, 211–12 (1986); United States v. Jacobsen, 466 U.S. 109, 120–21 (1984); United States v. Place, 462 U.S. 696, 706–07 (1983); Smith v. Maryland, 442 U.S. 735, 744–46 (1979); United States v. Miller, 425 U.S. 435, 442 (1976).

18. *Miller*, 425 U.S. at 442–43.

19. *Smith*, 442 U.S. at 744–46.

20. *Ciraolo*, 476 U.S. at 215.

able because it could be seen from an aircraft flying in public air space.[21] The property owners, thus, had no reasonable expectation of privacy.[22]

The Court later reflected on technology-assisted viewing in *Kyllo v. United States* and struck down the use of a heat sensor to detect marijuana cultivation inside a garage.[23] Justice Scalia said that when "the government uses a device that is not in general public use . . . [then it is] unreasonable without a warrant."[24] The Court distinguished the use of the heat sensor from a flyover, the method used in *California v. Ciraolo*, by stating that although the heat was emanating into public space, the public heat signature was detected by using a technology that was not "in general public use."[25] Because the heat signature was not generally accessible to the public, unlike air travel, the government needed a warrant as the heat signature was "private" information.[26]

As a result of these decisions, the meaning of "reasonable expectation of privacy" currently turns on whether and how technology is commercially deployed. The rapid development and distribution of tracking technologies used in daily life, ranging from social media infrastructure to cameras recording movements through public and private spaces, quite clearly impact whether activities will be treated as publicly available and whether anyone can reasonably expect privacy in their personal information.[27]

With the Court's definition of privacy only extending to that which we should reasonably expect to be private, mapping the third-party and plain-view doctrines to transaction records leaves little space for privacy. Technological evolution eviscerates any boundary of what we can reasonably expect to be private by upending social expectations with the deployment of personal technologies such as smartphones.[28] A few simple examples illustrate how information technology can be disruptive of social expectations. In 2001, the use of facial recognition scanning for every football fan entering the Super Bowl in Miami caused a stir.[29]

21. *Id.* at 213–14. The "plain-view" doctrine creates an exception to the Fourth Amendment warrant requirement for seizures. The doctrine relates to privacy expectations because of the consequences it assigns to publicly available information.

22. *Id.* at 214.

23. Kyllo v. United States, 533 U.S. 27, 40 (2001).

24. *Id.*

25. *Id.* at 33–34, 40.

26. *Id.*

27. *See* Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083, 1086–87 (2002) (Solove argues that the doctrine fails in the face of "digital dossiers," or aggregations of data that act as digital biographies).

28. *Id.* at 1085–1086.

29. *See* Declan McCullagh, *Call it Super Bowl Face Scan I*, WIRED (Feb. 2, 2001), http://www.wired.com/politics/law/news/2001/02/41571.

Mass scale public surveillance devices were not in general use at that time.[30] But today, facial recognition software is routinely embedded in portable computing devices, such as the face and optic recognition features in Apple's iPhoto software and the Samsung Galaxy S4 smart phone.[31] Personal drones cost less than $300 on Amazon, can stream live high-definition ("HD") video feeds to a smartphone or tablet,[32] and are now in general public use.[33] Cell phone routing requirements, as well as smartphone GPS functionality, mean that multiple parties (mobile phone providers, application providers, and cell tower owners, to name a few) each have tracking information on mobile phone users' movements.[34] Moreover, cell phones serve as small pervasive recording devices.[35] By December 2012, the number of active devices in the United States exceeded the national population.[36]

In light of these ubiquitous technologies, the limits of Justice Scalia's opinion for the Court in *Kyllo* become apparent. The Big Data project to constantly track and collect personal information[37] means there can be no such thing as an expectation of privacy. Information that is in plain view or publicly available, coupled with the third-party doctrine in this context, translates to no reasonable expectation of privacy in data. In the face of "ambient surveillance,"[38] how can any notion of a reasonable expectation of privacy survive? Even the notion that a boundary can be drawn around whether technology to assist discovering infor-

30. *Id.*

31. *See iPhoto '11: Faces Overview*, APPLE.COM, http://support.apple.com/kb/PH2369 (last modified Apr. 23, 2013) (describing the Faces feature); Agam Shah, *Inside Samsung Galaxy S4's Face and Eye-Tracking Technology,* COMPUTERWORLD (Mar. 15, 2013, 3:06 AM), http://www.computerworld.com/s/article/9237622/Inside_Samsung_Galaxy_S4_s_face_and_eye_tracking_technology.

32. *Parrot AR.Drone 2.0 Quadricopter*, AMAZON.COM, http://www.amazon.com/Parrot-AR-Drone-Quadricopter-Controlled-Android/dp/B007HZLLOK (last visited Aug. 27, 2014) (the device can be controlled by an iPhone, iPad, or Android device and can stream high-definition video to those devices).

33. *CBS 2 Investigation: Beware of Domestic Drones—The High-Flying Spies*, CBS NEW YORK (May 1, 2013, 11:04 PM), http://newyork.cbslocal.com/2013/05/01/cbs-2-investigation-beware-of-domestic-drones-the-high-flying-spies/.

34. *See, e.g.*, *Surveillance Self-Defense: Mobile Devices*, ELECTRONIC FRONTIER FOUND., https://ssd.eff.org/tech/mobile (last visited June 19, 2014).

35. Wendy Ruderman, *Is Someone Recording This? It's Harder to Find Out*, N.Y. TIMES (Apr. 7, 2013), http://www.nytimes.com/2013/04/08/nyregion/secret-recording-grows-safer-as-the-wire-grows-tinier.html.

36. *Annual Wireless Industry Survey*, CTIA.ORG, http://www.ctia.org/your-wireless-life/how-wireless-works/annual-wireless-industry-survey (last updated June 2014).

37. Kenneth Cukier, *Data, Data Everywhere*, ECONOMIST, Feb. 25, 2010, http://www.economist.com/node/15557443.

38. Seth F. Kreimer, *Pervasive Image Capture and the First Amendment: Memory, Discourse, and the Right to Record*, 159 U. PA. L. REV. 335, 347–54 (2011) (noting "ambient" image capture and the lack of a reasonable expectation of privacy for tort law).

mation is in general use or not in general use becomes irrelevant. Alternate data sources abound. For instance, just as grow lamps produce heat signatures that could not be obtained by heat sensors without a warrant, the lamps will also generate signature electrical use patterns.[39] As it turned out, the police in *Kyllo* had also obtained electric use records and matched them to grow lamp patterns.[40] Under the third-party doctrine, the police did not need a warrant to obtain this revealing information from the power company.

But this technological disruption of expectations is only part of the story. In other contexts, the Supreme Court approached information privacy differently. Rather than focus on the individual's expectation or "plain view," the Court focused on how technologically mediated access to information impacts the individual. For example, in *U.S. Department of Justice v. Reporters Committee for Freedom of the Press*, the Court denied access to a rap sheet, even though each item on the rap sheet was publicly available information.[41] The Court even upheld, against a First Amendment challenge, a purpose restriction limiting why someone could gain access to government-held personal information and restricting how that information could be used.[42] These issues of information access and use are also put in play by technological developments.

III. The Transformation of Information Flows and Constitutional Privacy Protection

The evolution of information technology has transformed data flows in ways that expose the fault lines of the constitutional approach to privacy protection. Information technologies have propelled this transformation of information flows through three stages of development: A) the obscurity of information available to the public; B) the accessibility of information to the public; and C) the transparency and publicity of information to the public. The movement through these stages creates an important transformation of privacy in public.

39. Nat'l Inst. of Standards and Tech., U.S. Dep't of Commerce, NISTIR 7628, Guidelines for Smart Grid Cyber Security: Vol. 2, Privacy and the Smart Grid 6 (2010), *available at* http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol2.pdf (smart grid technology "can recognize unique electric signatures for consumer electronics and appliances and develop detailed, time-stamped activity reports within personal dwellings").

40. United States v. Kyllo, 809 F. Supp. 787, 790 (D. Or. 1992) (these facts were discussed at the trial court level; the Supreme Court only focused on the heat sensor technology).

41. 489 U.S. 749, 753, 780 (1989) (denying access to a rap sheet even though each element on the sheet was public information).

42. L.A. Police Dep't v. United Reporting Publ'g, 528 U.S. 32, 34, 40 (1999).

A. *Stage 1: Obscurity and Privacy Expectations*

At the first stage, before the ubiquitous deployment of information technologies, obscurity of information provided an important degree of privacy protection.[43] As a practical matter, data that was inaccessible was private, and the public could have expectations of actual privacy, even if theoretically the information was available for scrutiny.[44] The Supreme Court in *United States v. Jones* acknowledged this reality: "In the pre-computer age, the greatest protections of privacy were neither constitutional nor statutory, but practical. Traditional surveillance for any extended period of time was difficult and costly and therefore rarely undertaken."[45]

While acknowledging the intrinsic privacy of obscure public records, the Court's view is inherently contradictory: if privacy were protected as a practical matter, then individuals had an expectation that should have been protected as a constitutional matter. In other words, obscurity plays a normative role in shaping social expectations of privacy that the Court would then have to protect.

B. *Stage 2: Accessibility and Privacy Expectations*

As technology develops, obscurity is eroded through the accessibility of personal information, and constitutional doctrine has a death struggle with expectations. The struggle derives first from the accessibility of personal information of anyone in public, or put another way, from the modern loss of anonymity in public. Before digital cameras could capture high-resolution images at great distances and computer algorithms could match photos with identities, individuals walking through public places, like Grand Central Terminal in New York City, at rush hour, would be anonymous in a crowd.[46] This anonymity existed even though the individuals were in plain view. Now, with surveillance cameras on

43. *See* Woodrow Hartzog & Frederic Stutzman, *The Case for Online Obscurity*, 101 CALIF. L. REV. 1, 5 (2013).

44. *Id.* at 9 ("online obscurity is a general expectation").

45. United States v. Jones, 132 S. Ct. 945, 963 (2012) (Alito, J., concurring).

46. *See, e.g.*, Charlie Savage, *Facial Scanning Is Making Gains in Surveillance*, N.Y. TIMES, Aug. 21, 2013, at A1, http://www.nytimes.com/2013/08/21/us/facial-scanning-is-making-gains-in-surveillance.html (describing the ability to link public video cameras with facial scanning); Sean Gallager, *Flying RoboCop is a "Riot Control" Octocopter with Guns and Lasers*, ARS TECHNICA (June 19, 2014, 2:34 PM), http://arstechnica.com/tech-policy/2014/06/flying-robocop-is-a-riot-control-octocopter-with-guns-and-lasers/ ("The Skunk is also equipped with FLIR thermal infrared and HD color cameras to capture the identity of those in a crowd to be controlled."); Michael B. Kelley, *The FBI's Nationwide Facial Recognition System Ends Anonymity as We Know It*, BUS. INSIDER (Sept. 10, 2012, 4:35 PM), http://www.businessinsider.com/the-fbis-nationwide-facial-recognition-system-2012-9 (reporting on FBI's $1 Billion Next Generation Identification program to deploy facial recognition throughout the U.S.).

every building and street corner, and with digital facial recognition capabilities in wide use on laptops and on social networks like Facebook,[47] society can no longer claim any expectation of anonymity in crowds. Alessandro Acquisti at Carnegie Mellon has even demonstrated on national television that an image of an unknown student walking across a college campus can readily be used to identify the individual, scrape personal information from the Internet, and reverse engineer the student's social security number.[48]

The ubiquity of image-capture devices in private hands also means that individuals lose an expectation of privacy in non-public places. Anyone in a non-public place now has the capacity to capture image and audio on a pocket smartphone and make those recordings accessible to the world through popular services such as YouTube and Tumblr. One company, Redpepper, is deploying cameras in places like bars and hotels in order to track those who patronize the establishments and has a partnership with Facebook to offer identified individuals special deals.[49] The system works by matching patrons' faces against the Facebook profiles of those who opted into the system.[50] However, even if an individual does not opt into the scanning, the technology is in place, and the establishment owner and Facebook can each know the name of every identified patron. Since this identification is made to a third party, the police would not need a warrant under the Fourth Amendment to know who was in the establishment.[51] In other words, what might have been a previously obscure, anonymous presence in a private place becomes an identified act.

The constant tracking of individuals' movements, whether in physical space via pocket tracking devices (cell phones) or on the Internet via transaction logging, makes personal information widely accessible. Multiple parties, such as telecommunications service providers, websites, and transaction partners, to name a few, have access to the reams of daily data. The same is now true of government-held public records. The digitization of these records, like real property records, that once existed only in musty basements of government buildings now makes them widely accessible.[52]

47. *See* Lee, *supra* note 3. R

48. "*Big Brother" Is Big Business?*, CBS NEWS (May 16, 2013), http://www.cbsnews.com/8301-18560_162-57584887/big-brother-is-big-business/.

49. Sharon Gaudin, *Can Facedeals Overcome 'Creepy' Factor?*, COMPUTERWORLD (Aug. 23, 2012, 3:13 PM), http://www.computerworld.com/s/article/9230548/Can_Facedeals_overcome_creepy_factor.

50. *Id.*

51. The third-party doctrine would apply to the identification of the individuals in the bar. *See supra* Part II.

52. *See, e.g.*, *Judicial Conference Privacy Subcommittee, Conference on Privacy and Internet*

The Supreme Court recognized that the broad accessibility of personal information creates a qualitative shift, but it could not frame the contours. In *Whalen v. Roe*, the Court considered a Fourteenth Amendment challenge to a New York state database program that required pharmacies to report physicians' narcotic prescriptions.[53] Justice Brennan wrote that "[t]he central storage and easy accessibility of computerized data vastly increase the potential for abuse,"[54] and Justice Stevens noted that "[w]e are not unaware of the threat to privacy implicit in the accumulation of vast amounts of personal information in computer data banks."[55] The case was pre-Internet, and yet the Court struggled with the impact of digitization and accessibility on its conceptualization of privacy.

C. *Stage 3: Transparency and Privacy Expectations*

Deployed technologies move the information flows beyond accessibility to transparency and its attendant publicity.[56] Collections of accessible personal information become transparent to the world through search technologies, push notification technologies, blogs, and hosting. As this occurs, the utility of the Fourth Amendment's "reasonable expectation of privacy" standard diminishes. Justice Sotomayor in her concurrence in *United States v. Jones* explicitly recognized this problem. She wrote: "[T]his approach is ill suited to the digital age, in which people reveal a great deal about themselves to third parties in the course of carrying out mundane tasks."[57]

Justice Sotomayor recognized that new social norms of sharing information on social networking sites are incompatible with the Fourth Amendment standard. Nonetheless, the Court responded to the challenge with a narrow decision on technical grounds. The police had put a physical device on the defendant's car without a valid warrant to monitor the defendant's movements on public streets over a period of time.[58] The Court determined that the police had committed a physical trespass on the defendant's property, like breaking into a home,[59] and avoided the real issue of information aggregations and transparency.

Access to Court Files, 79 FORDHAM L. REV. 1, 4–6 (statement of Joel R. Reidenberg).

53. 429 U.S. 589, 591 (1977).

54. *Id.* at 607.

55. *Id.* at 605.

56. *See generally* Hartzog & Stutzman, *supra* note 43, at 32–40. In their paper reflecting on a model for online obscurity, Hartzog and Stutzman's factors to determine if information is obscure map more closely to what I address here as accessibility and transparency of personal information.

57. United States v. Jones, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring).

58. *Id.* at 948.

59. *Id.* at 949.

In another much earlier context, however, the Supreme Court articulated that the transparency of citizens' personal information due to the ease of computer access to public records raised privacy concerns that were otherwise absent when those records were obscure and that computerized information warranted protection. In a landmark Freedom of Information Act case, the Court denied journalists access to police department rap sheets listing all of a person's arrests, even though each data point was public information.[60] The Court stated, "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."[61]

In deciding whether the Freedom of Information Act's privacy exemption permitted the police to withhold the data, the Court's analysis relied on the Fourth Amendment concept of a "reasonable expectation of privacy."[62] The Court essentially said that when discrete publicly available information was complied together and made transparent, it had a qualitatively different privacy character than the previously obscure, distinct parts.[63]

Similarly, the Supreme Court grappled with the expectations of privacy when New York state mandated that the narcotic prescription records of physicians be made transparent to specific state officials through a state database.[64] The New York statute was challenged as a Fourteenth Amendment violation, but the Court permitted the creation of the database where strict limits were placed by the state on access to the data so that the data would not be widely transparent.[65]

In the First Amendment context, two cases, one recent and one from fourteen years ago, struggled with the transparency and publicity of personal information arising in public contexts. Four years ago, in *Doe v. Reed*, members of a group in Washington state sought to block the disclosure of their names as signatories on a petition to require a statewide ballot referendum.[66] The petitioners' concern was that the

60. U.S. Dep't of Justice v. Reporters Comm. for Freedom of the Press, 489 U.S. 749, 753 (1989).

61. *Id.* at 764.

62. *Id.* at 780 (stating 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").

63. *Id.* at 764.

64. Whalen v. Roe, 429 U.S. 589, 598–604 (1977) (discussing whether the statute "invades a constitutionally protected 'zone of privacy' and holding that the patient-identification requirements of the statute do not invade "any right or liberty protected by the Fourteenth Amendment").

65. *Id.*

66. 130 S. Ct. 2811, 2815 (2010).

transparency and resulting publicity to their identities would cause them harm because of the unpopularity of their views.[67] The Court, however, upheld the disclosure of names and thus required that the personal information generated in the context of the ballot petition had to be transparent.[68] Yet previously, the Supreme Court was more sympathetic to blocking the transparency of arrestees' records. In *Los Angeles Police Department v. United Reporting Publishing*, the government released arrestee records only for limited uses by recipients.[69] The use limitations were challenged on First Amendment grounds, and the Court held that the limitations on transparency (i.e. banning use for any purpose) were constitutionally permissible where the government was not compelled to disclose any data in the first instance.[70]

These last decisions are, in effect, movements away from reasonable expectations of privacy and toward articulating appropriate levels of transparency to personal information gathered publicly. The technology-driven transformation of information flows thus calls into question how society can deal with the privacy of personal information emanating from the public sphere.

IV. The Democratic Necessity for Privacy in Public

Privacy is fundamental to constitutional democracy affecting a citizen's ability to participate in deliberative democracy and to engage in robust governing dialogues.[71] The transparency of personal information has a very significant impact on our constitutional democracy in two ways. First, and counterintuitively, transparency threatens constitutional democracy on both an individual and institutional level. But, second, transparency can also be a mixed benefit for the preservation of democratic values.

A. *The Transparency Threat to Democratic Values*

The Declaration of Independence articulates well that the function of constitutional democracy is the assurance of the inalienable rights to "life, liberty and the pursuit of happiness."[72] But, transparency of personal information undermines those key values.

67. *Id.* at 2820.

68. *Id.* at 2821.

69. 528 U.S. 32, 34 (1999).

70. *Id.* at 39–41.

71. *See, e.g.*, Neil Richards, *Intellectual Privacy*, 87 Tex. L. Rev. 387, 403–04 (2008) (arguing that privacy is essential to democratic values of free thought and expression); Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 Vand. L. Rev. 1609, 1647 (1999) (arguing that privacy standards are necessary for deliberative democracy).

72. *See* The Declaration of Independence para. 2 (U.S. 1776).

Privacy protects citizens from violence. Two online data mash-ups illustrate the risk of harm from the lack of privacy in public. The now defunct app "Girls Around Me" scraped pictures of women that were publicly available in real-time on the Internet from social networking sites and displayed those pictures on a smartphone map based on the geolocation tags embedded in the women's photos.[73] The app was perfect for stalking unsuspecting women. Similarly, another app, PleaseRobMe.com was a mash-up that used social media status updates to show maps in real time where vacant apartments were likely located.[74] The app would scrape the Internet for social network postings such as: "I'm going to school today" or "I'm at the Privacy Law Scholars Conference."[75] The app would search to match the poster's identity with available information on the individual's place of residence—all of which are publicly observable data points. The point of the developers was quite clear: to illustrate the great risks of transparency and publicity of information combinations.[76]

Privacy also enables citizens to hold and advocate unpopular ideas. Anonymous speech is protected in the United States.[77] Voting records are held confidential for this very reason.[78] Anonymity in public is a critical feature for an open society.[79]

Institutionally, privacy is essential to the integrity of the jury system. The transparency of personal information online takes juror research out of the structure and judicial supervision out of the voir dire process. Similarly, jurors tweeting and judges friending and posting on Facebook can raise significant issues for the public's confidence in the integrity of the judicial system.[80]

---

73. *See* Nick Bilton, *Girls Around Me: An App Takes Creepy to a New Level*, N.Y. TIMES BITS (Mar. 30, 2012, 4:43 PM), http://bits.blogs.nytimes.com/2012/03/30/girls-around-me-ios-app-takes-creepy-to-a-new-level/.

74. *See, e.g.*, Andrew Hough, *Please Rob Me Website Causes Fury for 'Telling Burglars When Twitter Users are Not Home'*, THE TELEGRAPH (Feb. 19 2010, 7:30 AM), http://www.telegraph.co.uk/technology/twitter/7266120/Please-Rob-Me-website-tells-burglars-when-Twitter-users-are-not-home.html; Ryan Kim, *PleaseRobMe.com Posts When You're Not at Home*, SFGATE (Feb. 18, 2010, 4:00 AM), http://www.sfgate.com/crime/article/PleaseRobMe-com-posts-when-you-re-not-at-home-3272742.php.

75. Kim, *supra* note 74. **R**

76. *Id.*

77. McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 357 (1995).

78. *See* James A. Gardner, *Anonymity and Democratic Citizenship*, 19 WM. & MARY BILL RTS. J. 927, 942–43 (2011).

79. *See* Christopher Slobogin, *Public Privacy: Camera Surveillance of Public Places and the Right to Anonymity*, 72 MISS. L.J. 213, 231–44 (2002).

80. *See* Joe Palazzolo, *Arkansas Defendant Saved by the Tweet*, WALL ST. J.L. BLOG (Dec. 8, 2011, 4:14 PM), http://blogs.wsj.com/law/2011/12/08/arkansas-defendant-saved-by-the-tweet/ (conviction overturned because juror tweeted during trial); *see also* Alex Ginsberg, *SI Judge is Red 'Faced'*, N.Y. POST (Oct. 15, 2009, 4:00 AM), http://www.nypost.com/p/news/local/staten_

B. *The Transparency Support for Democratic Values*

While publicity of personal information can threaten society's claims to "life, liberty and the pursuit of happiness," transparency can also be a tool to strengthen constitutional democracy. Transparency can make public officials perform their jobs better and be more accountable to the public. The accessibility of personal information helps law enforcement address crime and national security concerns. So just as the transparency of personal information can be a safety threat for individuals, it can also be a tool for government acting in its capacity of protecting citizens.

Publicity of personal information can also preserve democracy by supporting oversight of government. For example, the website OpenSecrets.org aggregates publicly filed records and publicizes campaign donations and politicians' voting histories. This enables citizens to see who is financing elected officials and how those officials may be influenced in their voting.

Similarly, the ubiquity of image-capture devices may be used to film police in action. This can provide a powerful public, visual check on any abuses of police power. Police have been disciplined for abuses based on citizen videos.[81] At the same time, police departments resist this form of oversight[82] and have actually charged people with crimes for filming police engaged in making arrests.[83] Courts by and large have ruled that filming police is constitutionally protected as an oversight function of the public.[84] The public can film the police so long as they are not impeding the officers' performance of their police functions.[85]

Public image capture, however, may also cross a fine line into vigilantism. For example, the Blue Servo network is a controversial network of cameras set up so that "[c]itizens can sign up as Virtual Texas Deputies[SM] to participate in border surveillance through this social network."[86] And Reddit was infamously used to falsely accuse a missing Brown University student of bombing the Boston Marathon.[87]

---

island/item_1TCZaxBoS2p5oOyES11jPN (judge disciplined for friending lawyers who were about to appear before him on Facebook).

81. *See, e.g.*, *Police Officers Pulled Off Street After YouTube Video Surfaces,* ABC 7 EYEWITNESS NEWS (Jan. 26, 2013, 6:56 PM), http://7online.com/archive/8969480/.

82. Smith v. City of Cumming, 212 F.3d 1332, 1333 (11th Cir. 2000).

83. *See, e.g.*, Glik v. Cunniffe, 655 F.3d 78, 79 (1st Cir. 2011).

84. *Smith*, 212 F.3d at 1333.

85. *Glik*, 655 F.3d at 84.

86. *About BlueServo*, BLUESERVO, https://web.archive.org/web/20130626055913/http://www.blueservo.net/about.php (last visited Sept. 18, 2014) (accessed by searching for BlueServo in the Internet Archive index).

87. Bill Briggs & Bob Sullivan, *Missing Brown University Student's Family Dragged into Virally Fueled False Accusation in Boston*, NBC NEWS (Apr. 19, 2013, 11:20 AM), http://usnews.

In short, a lack of privacy for information observed in public areas both threatens and preserves the key values of a constitutional democracy.

V. FINDING "PRIVACY IN PUBLIC"

The recreation of privacy in public suggests that the "reasonable expectation of privacy" standard needs to give way to a standard that takes into consideration a variant of what Helen Nissenbaum coins as "contextual integrity."[88]

The variant is to examine the generation of personal information in order to distinguish between observable acts that are "non-public," or private-regarding, and those that are of public significance, or "governance-related."[89] 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.[90] 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.[91] Applying a public significance filter to the transparency and publicity of personal information seems promising as a means to restore privacy in public. Drawing the distinction is thus an important task.

A. *Private-Regarding Acts*

The *Katz* decision provides a useful starting point to identify "private"-regarding acts. Even though the phone call in that case took place in a publicly observable place on a street corner,[92] 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

nbcnews.com/_news/2013/04/19/17826915-missing-brown-university-students-family-dragged-into-virally-fueled-false-accusation-in-boston.

88. *See* HELEN NISSENBAUM, PRIVACY IN CONTEXT 127 (Stanford Univ. Press 2010). *See generally* Andrew D. Selbst, *Contextual Expectations of Privacy*, 35 CARDOZO L. REV. 643 (2013) (arguing that Nissenbaum's theory of contextual integrity should be applied to Fourth Amendment analysis).

89. *See* NISSENBAUM, *supra* note 88, at 127–55.

90. 491 U.S. 524, 526 (1989).

91. *Id.* at 541.

92. Katz v. United States, 389 U.S. 347, 348 (1967).

addressed in *Whalen v. Roe*[93] 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.[94] 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.

B. *Governance-Related Acts*

To qualify as a "governance act," the action or activity needs to have an inherent public significance. Samuel Warren and Louis Brandeis foreshadowed this approach when they first argued that privacy should not attach to matters of "public or general interest" or to matters that "have no legitimate connection to fitness for public office."[95] An individual's subjective intent does not thus determine whether an observable activity in a public place is "governance-related." Rather, the social norm of public significance and public interest set the boundaries of "governance-related" information. This public significance test parallels similar distinctions in tort law. Defamation law distinguishes between public and private figures on the basis of public interest.[96] Likewise, the tort for publication of private facts is unavailable when the private facts are of public importance.[97]

Contrast *Katz* and *Whalen*, with *Doe v. Reed*.[98] In the *Reed* case, a group of Washington state citizens signed a petition to hold a referendum seeking to overturn a state statute expanding civil rights for same-sex domestic partners.[99] The signatories to the petition sought to block the disclosure of their names to the proponents of same-sex rights.[100] The act of signing the petition appears quite clearly as a publicly significant act—a governance act. The signatories are engaging in a collective governance act by fulfilling the prerequisites for a plebiscite—securing a certain number of signatures of qualified voters. Further, the signatories are also petitioning for an act of government—a ballot question for the citizens to supplant the legislature's decision. These activities, collectively, would be characterized as a "governance act." Under the gov-

93. Whalen v. Roe, 429 U.S. 589, 593 (1977).

94. *Id.*

95. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 214, 216 (1890).

96. N.Y. Times Co. v. Sullivan, 376 U.S. 254, 272–73 (1964).

97. RESTATEMENT (SECOND) OF TORTS § 652D(b) (1977).

98. 130 S. Ct. 2811 (2010).

99. *Id.* at 2815.

100. *Id.*

ernance rationale, the result would be the same as the Court's decision in *Doe*.

Because public significance is not always binary and may vary with context, information may be "governance-related" only for certain situations. For example, the arrest records in *Reporter's Committee*[101] are of public significance and thus clearly "governance-related" for purposes of the justice system and public oversight, but are not necessarily "governance-related" when sought to be used outside the justice system in combination with other information. Similarly, real property records are of public significance for real estate transactions but not of public significance for the commercialization of innumerable products. Here, the relationship to governance turns on the use of the publicly available information for a purpose that has inherently public importance.

C. *Complex Acts*

Nuances in the distinction between private- and governance-related acts play out in the *United States v. Jones* case.[102] In *Jones*, the police placed a tracking device on Jones' car and recorded his movements on a public street.[103] The same information could have been obtained from Jones' cell phone provider or from street surveillance cameras.[104] The observable movement on a public street is a governance-related act—observation indicates if the driver is observing traffic rules. This moment of instant scrutiny is of public significance. However, the capture of the movements to profile the driver crosses into the private habits and associations of the driver.[105] The profile can reveal whether an individual visits a doctor, an unpopular political figure, or a family member. The profile is not a "governance-related" compilation or an act of inherent public significance like the behavior of the petition signatories in *Doe v. Reed* to get a measure on the ballot.[106] This distinction goes to the worry that Justice Sotomayor expressed in her concurrence in *Jones* about aggregations of information.[107]

D. *First Amendment Considerations*

The private-regarding/governance-related approaches raise three

101. U.S. Dep't of Justice v. Reporters Comm. for Freedom of the Press, 489 U.S. 749, 753 (1989).

102. 132 S. Ct. 945 (2012).

103. *Id.* at 948.

104. *Id.* at 950.

105. *See* Dorothy J. Glancy, *Privacy on the Open Road*, 30 OHIO N.U. L. REV. 295, 295–96 (2004) (discussing privacy interests and road surveillance).

106. *See* 130 S. Ct. 2811, 2815 (2010).

107. *Jones*, 132 S. Ct. at 955–56 (Sotomayor, J., concurring).

important First Amendment considerations that can be addressed by the public significance metric. First, journalistic uses of information available in public are preserved. Newsworthiness will invariably take an activity in public from a private matter to one of public significance. For example, an individual's photograph taken on a public street and used to illustrate a news story would be considered "of public interest" just as such uses are denied privacy tort protection.[108]

Second, direct recipients of private-regarding information could still use the information. For example, someone on the street who overheard a pedestrian in conversation on a cell phone might be able to repeat or report on what was overheard. While the cell phone conversation would ordinarily be considered a private matter and not one of public significance, the speaker is publicizing information to nearby listeners and turning a private-regarding act into something of limited public significance. Just as the privacy tort protection against publication of private facts becomes unavailable when an individual publicizes otherwise private facts,[109] here a private-regarding act can acquire some public significance. The scope of the public interest, though, should be constrained. For example, if the listener were recording the street conversation, the public significance would not justify posting the recording to a popular website like YouTube for widespread dissemination or to sell the recording.[110]

And, third, government surveillance would not be empowered. Private-regarding acts would be constitutionally protected as freedom of association.[111] At the same time, surveillance of governance-related acts, like a public protest, would not be affected and would only be restricted to the extent that the First Amendment protects anonymous political activity.[112]

VI. CONCLUSION

As information changes from obscure, to accessible, to transparent, the United States will have to confront the disruptive impact of information technology on established approaches to privacy. At the moment,

108. *See* Ault v. Hustler Magazine Inc., 860 F.2d 877, 883 (9th Cir. 1988); Arrington v. N.Y. Times Co., 434 N.E. 2d 1319, 1323–24 (N.Y. 1982).

109. *See* RESTATEMENT (SECOND) OF TORTS § 652D(b) (1977).

110. Note that this would not be the case if the speaker were a public figure in his or her own right such as a politician.

111. *See generally* NAACP v. Alabama *ex rel.* Patterson, 357 U.S. 449, 458–62 (1958) (holding that members of the NAACP may not be compelled to disclose their association with the union to the State).

112. *See* Church of the Am. Knights of the Ku Klux Klan v. Kerik, 356 F.3d 197, 210 (2d Cir. 2004) (upholding a New York statute limiting masked protest).

the Supreme Court is poised to confront how it will deal with aggregations of information that are readily available from public observation because of technology or, as Justice Sotomayor put it, our mundane activities.[113]

Perhaps the clothing designer Carlton Yaito captured this new sense of need in society when he described his new brand of clothing, *Privacy in Public*: "The concept of Privacy In Public is based on you as an individual. Put yourself in a situation where [you're] surrounded by dozens of people, suddenly you drift off into your own world. Not realizing everything around you. That is Privacy In Public."[114]

In short, we must always recall Justice Stewart's famous words in *Katz*, "the Fourth Amendment protects people, not places."[115]

113. United States v. Jones, 132 S. Ct. 945, 947 (2012) (Sotomayor, J., concurring).

114. *About Privacy in Public*, PRIVACY IN PUBLIC, http://privacyinpublic.com/about.php (last visited Sept. 3, 2014).

115. Katz v. United States, 389 U.S. 347, 351 (1967).