2015

Regulating Real-World Surveillance

Margot E. Kaminski
University of Colorado Law School

REGULATING REAL-WORLD SURVEILLANCE

Margot E. Kaminski*

Abstract: A number of laws govern information gathering, or surveillance, by private parties in the physical world. But we lack a compelling theory of privacy harm that accounts for the state's interest in enacting these laws. Without a theory of privacy harm, these laws will be enacted piecemeal. Legislators will have a difficult time justifying the laws to constituents; the laws will not be adequately tailored to legislative interest; and courts will find it challenging to weigh privacy harms against other strong values, such as freedom of expression.

This Article identifies the government interest in enacting laws governing surveillance by private parties. Using social psychologist Irwin Altman's framework of "boundary management" as a jumping-off point, I conceptualize privacy harm as interference in an individual's ability to dynamically manage disclosure and social boundaries. Stemming from this understanding of privacy, the government has two related interests in enacting laws prohibiting surveillance: an interest in providing notice so that an individual can adjust her behavior; and an interest in prohibiting surveillance to prevent undesirable behavioral shifts.

Framing the government interest, or interests, this way has several advantages. First, it descriptively maps on to existing laws: These laws either help individuals manage their desired level of disclosure by requiring notice, or prevent individuals from resorting to undesirable behavioral shifts by banning surveillance. Second, the framework helps us assess the strength and legitimacy of the legislative interest in these laws. Third, it allows courts to understand how First Amendment interests are in fact internalized in privacy laws. And fourth, it provides guidance to legislators for the enactment of new laws governing a range of new surveillance technologies—from automated license plate readers (ALPRs) to robots to drones.

---

* Assistant Professor of Law at the Ohio State University Moritz College of Law. Thanks to BJ Ard, Lisa M. Austin, Derek Bambauer, Jane Bambauer, Michael Birnhack, Marc J. Blitz, Kiel Brennan-Marquez, Julie Cohen, Ruth Colker, Woodrow Hartzog, Dennis Hirsch, Karen Levy, William McGeveran, Neil Richards, David Vladeck, and Jonathan Zittrain (for enabling an early-stage discussion of this project at the Berkman Center for Internet & Society at Harvard University); attendees at the Midwestern Privacy Scholars Conference; Michael Birnhack's students at Tel Aviv University; attendees at my Berkman Center talk on this topic in 2014; and attendees and participants at Privacy Law Scholars Conference 2014. As always, many thanks to Matthew Cushing for tolerating my increasing fascination with drones.

INTRODUCTION

Privacy is situated; it exists in context. That context can have physical, social, and temporal dimensions. While a growing number of scholars have discussed the importance of context to surveillance online, it often gets neglected in the physical world.[1] Courts oversimplify

1. For explorations of context online, see, for example, HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE (2010) (outlining Nissenbaum's theory of contextual integrity); Woodrow Hartzog & Frederic Stutzman, *The Case for Online Obscurity*, 101 CALIF. L. REV. 1 (2013) (discussing online privacy as relative levels of obscurity); Lior Jacob Strahilevitz, *A Social Networks Theory of Privacy*, 72 U. CHI. L. REV. 919 (2005) (discussing the social context of disclosure online); Katherine J. Strandburg, *Home, Home on the Web and Other Fourth Amendment Implications of Technosocial Change*, 70 MD. L. REV. 614 (2011) (discussing cloud computing and social networking as technosocial extensions of real spaces like the home).

physical context, characterizing a situation as private if it takes place in the home, and public if it takes place outside. But in practice, surveillance subjects in the physical world rely on and use detailed temporal, social, and physical features of their environment when calculating their ideal degree of disclosure to others at a given moment.

When the introduction of new surveillance technologies undermines features of the physical environment that people once relied on in calculating their degree of privacy or openness, the state may intervene. For example, celebrities once relied on physical distance and physical walls to keep out snooping paparazzi. When paparazzi started using visual and auditory enhancing technologies to overcome both distance and walls, California enacted a paparazzi law to protect individuals from a "constructive invasion of privacy" through the use of a "visual or auditory enhancing device."[2] In 2014, California amended this law to expand its coverage to constructive privacy intrusions by "any device" in order to reach aerial surveillance by drones.[3]

Surveillance technologies from video cameras to drones have inspired the enactment of a number of laws governing surveillance by private parties in real physical space. These laws have received surprisingly little in-depth analysis as a category.[4] This Article brings these laws together under one umbrella and proposes a way to understand the government's interest in enacting them.

The government has an interest in protecting privacy. But merely

---

2. *See* Act of Sept. 30, 1998, 1998 Cal. Legis. Serv. Ch. 1000 (codified as amended at CAL. CIV. CODE § 1708.8(b) (West, Westlaw through 2015 Reg. Sess.)).

3. *See* Assemb. 2306, 2013–2014 Reg. Sess. (Cal. 2014), *available at* http://leginfo.ca.gov/pub/13-14/bill/asm/ab_2301-2350/ab_2306_bill_20140930_chaptered.pdf; DL Cade, *California Updates Invasion of Privacy Law to Ban the Use of Camera Drones*, PETAPIXEL (Oct. 14, 2014), http://petapixel.com/2014/10/14/california-passes-law-banning-drones-protect-general-publics-privacy/.

4. A number of these laws have been addressed as individual topics. *See, e.g.*, Jesse Harlan Alderman, *Police Privacy in the iPhone Era?: The Need for Safeguards in State Wiretapping Statutes to Preserve the Civilian's Right to Record Public Policy Activity*, 9 FIRST AMEND. L. REV. 487 (2011); Erwin Chemerinsky, *Protecting Privacy From Technological Intrusions*, 1999 ANN. SURV. AM. L. 183 (2000); Michael Potere, Comment, *Who Will Watch the Watchmen?: Citizens Recording Police Conduct*, 106 NW. U. L. REV. 273 (2012); Travis S. Triano, Note, *Who Watches the Watchmen? Big Brother's Use of Wiretap Statutes to Place Civilians in Timeout*, 34 CARDOZO L. REV. 389 (2012); Nancy Danforth Zeronda, Note, *Street Shootings: Covert Photography and Public Privacy*, 63 VAND. L. REV. 1131 (2010).

Several scholars have addressed image capture more holistically, but from a First Amendment perspective. *See, e.g.*, Jane Bambauer, *Is Data Speech?*, 66 STAN. L. REV. 57 (2014); Ashutosh Bhagwat, *Producing Speech*, WM. & MARY L. REV. (forthcoming 2015); Seth F. Kreimer, *Pervasive Image Capture and the First Amendment: Memory, Discourse, and the Right to Record*, 159 U. PA. L. REV. 335 (2011).

identifying the government interest in surveillance laws as an interest in privacy protection is inadequate because privacy can mean many different things. The understanding of privacy behind legislation can greatly affect the scope of that legislation, and the ability of the government to justify it to constituents and in court.

This Article asks what theory of privacy drives the government to protect individuals from having information about them gathered by private, nongovernmental actors. Without a theoretical understanding of why these laws exist, arguments over whether they should exist at all will continue to be had on a case-by-case basis. This has led to piecemeal legal protection.[5] Legislators will find it easier to decide when such laws are necessary if they can better identify and discuss the government interests at stake. Understanding the government interest is crucial for making decisions about both when to enact these laws, and when these laws can withstand balancing against other values, such as freedom of expression.

In the 1970s, social psychologist Irwin Altman conceived of privacy as boundary management:[6] the process of dynamically managing the degree of disclosure of one's self to others. Privacy is not a single state of being; it is a process of calibration set in physical, social, and temporal space. Altman's great insight is that when a physical space changes, a person's ideal degree of disclosure does not necessarily change with it. So if a wall functionally disappears because of a new surveillance technology, a person who once relied on it for protection from disclosure may now start changing her behavior, to maintain the same desired degree of disclosure that existed when the wall protected her.

Building on this conception of privacy, this Article proposes that the government has a two-pronged interest in enacting surveillance laws to govern private actors. First, it has an interest in providing notice to individuals, both to let them recalibrate their ideal level of disclosure and to encourage governance of surveillance through social norms. Second, the government has an interest in preserving some situations as surveillance-free, to prevent undesirable behavioral shifts.

Understanding the government interest this way descriptively maps

---

5. Helen Nissenbaum, *Protecting Privacy in an Information Age: The Problem of Privacy in Public*, 17 J.L. & PHIL. 559, 565 (1998) (observing that "the absence of a clearly articulated philosophical base is not of theoretical interest only, but is at least partially responsible for the inconsistencies, discontinuities and fragmentation, and incompleteness in the framework of legal protections and in public and corporate policy").

6. *See generally* IRWIN ALTMAN, THE ENVIRONMENT AND SOCIAL BEHAVIOR (1975).

on to the laws legislators have in fact been enacting. A number of surveillance laws provide notice to an individual so she can optimize disclosure calibration, while other laws preserve certain situations as surveillance-free. Understanding the government interest in surveillance laws as an interest in boundary management should enable legislators to thoughtfully enact new laws and enable courts to better assess the strength of the privacy interest at stake.

The privacy interests at stake in these laws will soon be weighed against an interest in free speech.[7] Courts will soon need to assess surveillance laws for their compatibility with freedom of expression, as courts of appeals recognize a burgeoning First Amendment "right to record."[8] While the outcome of this balancing is outside the scope of this Article, a theory of the privacy interest at stake in surveillance laws can help courts assess when the interest is strongest, and when it is weaker. It can also help courts identify when privacy protection in fact enhances First Amendment interests, rather than conflicts with them. This Article shows that First Amendment interests are often internalized on the privacy side of the equation. Protecting privacy does not always conflict with the First Amendment; privacy protection often enables expression.

This Article begins by identifying technologies governed by surveillance laws, ranging from cameras to cellphones to drones to robots. It discusses several theoretical understandings of privacy, which have been used to describe the government interest in privacy lawmaking. It outlines Altman's theory of privacy as boundary management, and explains the government interests that the boundary management framework reveals. It addresses potential criticisms of the boundary management framework, and then identifies its benefits, including descriptive accuracy illustrated through a number of existing laws.

As new surveillance technologies increasingly come into public use, legislators will look to laws of the past to govern privacy problems of

---

7. In a forthcoming Article, I discuss the First Amendment side of this equation. A draft version of this forthcoming Article was workshopped at the 2015 Freedom of Expression Scholars Conference at Yale Law School. Margot E. Kaminski, *Privacy and the Right to Record* (forthcoming 2016) (formerly titled *Context, Barriers, and the Right to Record*).

8. A number of courts of appeals have recently recognized a "right to record." *See* Am. Civil Liberties Union of Ill. v. Alvarez, 679 F.3d 583, 595 (7th Cir. 2012); Glik v. Cunniffe, 655 F.3d 78, 83 (1st Cir. 2011) ("Our recognition that the First Amendment protects the filming of government officials in public spaces accords with the decisions of numerous circuit and district courts."); Kelly v. Borough of Carlisle, 622 F.3d 248, 262 (3d Cir. 2010); Smith v. City of Cumming, 212 F.3d 1332, 1333 (11th Cir. 2000) ("[W]e agree with the Smiths that they had a First Amendment right, subject to reasonable time, manner and place restrictions, to photograph or videotape police conduct.").

the very near future. Drones—with their ability to record individuals in public, from new vantage points, and at lower cost—are one technology driving the enactment of new privacy laws. The Federal Aviation Administration (FAA) has proposed its rules for commercial use of drones, and those rules are less restrictive than expected.[9] In the absence of a federal privacy regime, states will enact new laws to govern private parties' use of drones as a recording technology. This Article puts these laws in historical and theoretical context, and provides guidance for the enactment of future laws.

I. TECHNOLOGICAL AND SOCIAL CHANGES INSPIRE LEGAL EVOLUTION

Privacy laws are driven by social and technological change. As technologies evolve, legislators enact new laws. This Part gives an overview of some techno-social evolutions that have inspired the enactment of laws governing surveillance by private parties.

When Samuel Warren and Louis Brandeis wrote their seminal article on privacy in 1890, they were spurred by the fear of ubiquitous, intrusive recording devices: cameras.[10] Cheap, portable cameras could surreptitiously capture portraits and other private information. Warren and Brandeis were also motivated by social change. Popular journalism was booming, and there was a growing market for gossip.[11] This combination of social and technological change spurred Warren and Brandeis to propose a privacy right of action.

Other technological and social change inspired other laws. Morse's first telegraph was sent in 1844[12] and Edison's telephone was improved

---

9. Aaron Cooper, *FAA Proposes to Allow Commercial Drone Use*, CNN, http://www.cnn.com/2015/02/15/politics/drones-faa-rules-commercial-flights/ (last updated Feb. 15, 2015, 3:00 PM). The President recently ordered the National Telecommunications and Information Administration to engage in standards-setting around a voluntary privacy standard for commercial drone use by U.S. companies. BARACK OBAMA, PRESIDENTIAL MEMORANDUM: PROMOTING ECONOMIC COMPETITIVENESS WHILE SAFEGUARDING PRIVACY, CIVIL RIGHTS, AND CIVIL LIBERTIES IN DOMESTIC USE OF UNMANNED AIRCRAFT SYSTEMS (2015), *available at* www.whitehouse.gov/the-press-office/2015/02/15/presidential-memorandum-promoting-economic-competitiveness-while-safegua.

10. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 195 (1890) ("Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that 'what is whispered in the closet shall be proclaimed from the house-tops.'").

11. *Id.* at 196. Warren and Brandeis refer to an intrusive press "overstepping . . . bounds of propriety and of decency." *Id.*

12. LEWIS COE, THE TELEGRAPH: A HISTORY OF MORSE'S INVENTION AND ITS PREDECESSORS IN THE UNITED STATES 32 (1993).

in 1877.[13] Wiretapping and bugging technologies were developed shortly thereafter; the first police wiretap was in 1890.[14] These technologies, and the widespread adoption of the telephone, eventually drove the enactment of both state and federal privacy wiretapping and eavesdropping laws.[15]

A number of newer technologies enable sense-enhancement or super-human-like powers. Infrared sensors, heat sensors, and new powerful radar systems all allow people (mainly police) to "see" through walls.[16] Facial recognition and automated license plate readers enable the large-scale capture of information, tracking of individuals and their vehicles, and correlation of that information with information housed in massive databases.[17] Widespread adoption of Global Positioning System (GPS) technology has also driven extensive legal debate, culminating in a recent Supreme Court case and state laws.[18] Mobile carriers also track cellphone user movements, and "stingrays" or cell site simulators allow operators to directly access the location of cell phone users by mimicking cell towers.[19] Cell site tracking has received legislative and

---

13. GEORGE B. PRESCOTT, BELL'S ELECTRIC SPEAKING TELEPHONE: ITS INVENTION, CONSTRUCTION, APPLICATION, MODIFICATION AND HISTORY iv (1884).

14. For a history of wiretapping, see generally JAMES G. CARR, THE LAW OF ELECTRONIC SURVEILLANCE (1994); WHITFIELD DIFFIE & SUSAN LANDAU, PRIVACY ON THE LINE: THE POLITICS OF WIRETAPPING AND ENCRYPTION (1998); PRISCILLA M. REGAN, LEGISLATING PRIVACY: TECHNOLOGY, SOCIAL VALUES, AND PUBLIC POLICY (1995); ROBERT ELLIS SMITH, BEN FRANKLIN'S WEB SITE: PRIVACY AND CURIOSITY FROM PLYMOUTH ROCK TO THE INTERNET (2000).

15. *See, e.g.*, Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended at 18 U.S.C. §§ 2510–2521 (2012)); Act of March 25, 1987, 1986 Ohio Laws 457 (codified as amended at OHIO REV. CODE ANN. §§ 2933.51–.59 (West, Westlaw through 2015)).

16. Kyllo v. United States, 533 U.S. 27, 36 (2001) (holding that police use of thermal imaging to "see" into a house was unconstitutional under the Fourth Amendment); *see also* United States v. Denson, 775 F.3d 1214, 1218 (10th Cir. 2014) (noting that "the government brought with it a Doppler radar device capable of detecting from outside the home the presence of 'human breathing and movement within'"); Brad Heath, *New Police Radars Can "See" Inside Homes*, USA TODAY (Jan. 20, 2015, 1:27 PM), http://www.usatoday.com/story/news/2015/01/19/police-radar-see-throughwalls/22007615/.

17. *See, e.g.*, Laura K. Donohue, *Technological Leap, Statutory Gap, and Constitutional Abyss: Remote Biometric Identification Comes of Age*, 97 MINN. L. REV. 407, 410 (2012) (explaining that uses of facial recognition technologies "range from confirming targets for elimination and pairing photographs and data from different databases, to monitoring individuals as they move through public space").

18. United States v. Jones, __ U.S. __, 132 S. Ct. 945 (2012); H.R. 0603, 63d Leg., Reg. Sess. (Mont. 2013).

19. *Stingray Tracking Devices: Who's Got Them?*, ACLU, https://www.aclu.org/maps/stingray-tracking-devices-whos-got-them (last visited Sept. 5, 2015).

judicial attention.[20]

Unmanned aircraft systems (UAS), or drones, have shrunk in size, and lowered in cost in the past few years.[21] The increase in small drone use by hobbyists, and anticipated increase in drone use by commercial entities, has inspired states to enact a number of laws governing information capture by drones.[22] Drones are cheaper than helicopters, easier to operate, and provide a different vantage point than cellphone cameras. They also can capture information continuously, rather than at the behest of a user.

The much-anticipated rise of the Internet of Things—that is, a range of interconnected devices with sensors in the home, such as smart refrigerators—may inspire a range of new privacy laws. The Internet of Things will place eyes in the home, and create far more pervasive surveillance than exists even with today's extensive cellphone usage. Household robots may eventually raise similar privacy challenges, giving third party companies a window into locations to which they never had access.[23] As discussed at greater length in Part V.D., robots may also create new challenges due to anthropomorphic characteristics.[24] People may end up trusting their robots, caring for them, and consequently revealing more information than they would to a threatening-looking camera.

II. THEORIES OF PRIVACY AND INFORMATION GATHERING

In reaction to new technologies, states have enacted a range of laws governing surveillance in the physical environment.[25] Some of these

---

20. *See, e.g.*, Annabelle Steinhacker & Rubin Sinins, *New Jersey High Court Correctly Rules Cell Phone Locations Are Constitutionally Protected*, JURIST (Oct. 21, 2013, 10:17 PM), http://jurist.org/sidebar/2013/10/steinhacker-sinins-NJ-cell-tracking.php.

21. *See Hearing on Using Unmanned Aerial Systems Within the Homeland: Security Game Changer?: Hearing Before the Subcomm. on Oversight, Investigations, & Mgmt. of the H. Comm. on Homeland Sec.*, 112th Cong. (2012) (testimony and statement of Amie Stepanovich, Association Litigation Counsel, Electronic Privacy Information Center), *available at* http://homeland.house.gov/sites/homeland.house.gov/files/Testimony-Stepanovich.pdf.

22. M. Ryan Calo, *The Drone as Privacy Catalyst*, 64 STAN. L. REV. ONLINE 29 (2011), http://www.stanfordlawreview.org/online/drone-privacy-catalyst.

23. *See generally* Margot E. Kaminski, *Robots in the Home: What Will We Have Agreed To?*, 51 IDAHO L. REV. 661 (2015).

24. Ryan Calo, *Robotics and the Lessons of Cyberlaw*, 103 CALIF. L. REV. (forthcoming 2015); Kate Darling, *Extending Legal Rights to Social Robots* (April 23, 2012) (unpublished manuscript), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2044797 (arguing that because people tend to anthropomorphize robots, we should consider granting some kinds of legal protections to robots).

25. *See infra* Part V.A.

laws criminalize surveillance, while others provide a private right of action. These laws can be characterized as restrictions or prohibitions on surveillance; they govern the act by which information is collected.[26] But the government does not have a uniform interest in preventing all private information gathering, and diverse government interests are reflected in the diversity of the laws. The laws are tailored to particular technologies, such as zoom lenses, or to protect against particular harms, such as listening in on and recording a conversation. This suggests that legislatures understand that there is a range of government interests in preventing private actor surveillance.

Historically, a number of surveillance laws have been aimed at intrusive behavior by the media or others. These laws have been subject to little theoretical analysis for two reasons. First, the quintessential prohibition on private-actor surveillance is one of the oldest, best-established, and least-challenged privacy laws: the privacy tort of intrusion upon seclusion.[27] Second, most recent theorizing around privacy has addressed the puzzles raised by big data, focusing on what restrictions to place on data processing, not the moment at which data are gathered.[28] But many data analytics companies are now pursuing business models that rely on actively gathering information in the physical world rather than using information provided by others or gathered online.[29] This brings legislators back to the older question of how to govern surveillance, or information gathering, that takes place in the physical world.

The earliest such laws—the eavesdropping nuisance, Peeping Tom laws, and the tort of intrusion upon seclusion—could be justified as protecting a very modest understanding of privacy: privacy as physical withdrawal from the world. These early laws at their essence protect agreed-upon private spaces. While intrusion upon seclusion can be applied outside of the home, courts have often struggled in its

---

26. DANIEL J. SOLOVE, UNDERSTANDING PRIVACY 10–11, 106–07, 161–64 (2008) (classifying such laws as governing information collection by surveillance and intrusion).

27. RESTATEMENT (SECOND) OF TORTS § 652B (1977).

28. Helen Nissenbaum, Woodrow Hartzog, Danielle Citron, and Frank Pasquale, to name only a few, have been writing in this area. *See, e.g.*, NISSENBAUM, *supra* note 1; Danielle Keats Citron & Frank Pasquale, *The Scored Society: Due Process for Automated Predictions*, 89 WASH. L. REV. 1 (2014); Hartzog & Stutzman, *supra* note 1.

29. For example, some private companies use license plate readers to create databases that they then sell to other companies and law enforcement. *See, e.g.*, Steve Orr, *License Plate Data Is Big Business*, USA TODAY (Nov. 2, 2014, 5:13 PM), http://www.usatoday.com/story/news/nation/2014/11/02/license-plate-data-is-big-business/18370791/.

application, and repeatedly avowed that there is no privacy in public.[30]

A number of scholars have offered new theories of privacy, in contrast to this idea of privacy as complete withdrawal from the public world.[31] Because conceiving of privacy as withdrawal fails to account for any expectation of privacy in public, these scholars saw a need to develop a theory of privacy harm that could justify protection of privacy outside of the home. Thus they devised newer theories of privacy to justify the protection of privacy in public. But these theories neglect to link protection of privacy in public to protection of privacy in private, ignoring justifiable intuitions that there is a strong government interest in protecting against surveillance conducted in private places. In other words, to escape the public-private binary, they disembody privacy from the physical environment. This is a mistake.

This Part begins by discussing courts' frequent conceptualization of private and public as opposites, or a binary, with no overlap in between. It then turns to several of the scholars who have re-theorized privacy to address governance of privacy in public. It concludes by examining the limitations of these newer privacy theories as applied to information-gathering laws.

A. Privacy as Withdrawal into Private Spaces

Intrusion upon seclusion protects a particularly uncontroversial vision of privacy, one that is clearly understandable to most people: privacy as solitude or withdrawal. Not much ink needs to be spilled arguing for a theory of privacy harm that permits governments to protect individuals from having their solitude disrupted.[32] If you understand the purpose of privacy protection to be to protect an individual's ability to withdraw to private spaces, then the intrusion tort intuitively makes sense.

---

30. *See, e.g.*, Nader v. Gen. Motors Corp., 255 N.E.2d 765, 771 (N.Y. Ct. App. 1970) ("[I]t is manifest that the mere observation of the plaintiff in a public place does not amount to an invasion of his privacy."); Nussenzweig v. DiCorcia, No. 108446/05, 2006 WL 304832 (N.Y. Sup. Ct. Feb. 8, 2006) (finding that plaintiff failed to state a cause of action for a privacy claim over art photographs taken in a public street); McNamara v. Freedom Newspapers, Inc., 802 S.W.2d 901, 904 (Tex. App. 1991) (finding no invasion of privacy and strong First Amendment interests "[w]hen an individual is photographed at a public place for a newsworthy article and that photograph is published"); Shulman v. Grp. W Prods., 955 P.2d 469, 490 (Cal. 1988) ("[T]here is no liability for the examination of a public record concerning the plaintiff. . . . [Or] for observing him or even taking his photograph while he is walking on the public highway . . . ." (quoting RESTATEMENT (SECOND) OF TORTS § 652B, cmt. c. (1977))); Aisenson v. Am. Broad. Co., 269 Cal. Rptr. 379, 388 (Ct. App. 1990) (finding of filming in a public street that any invasion of privacy was "extremely de minimis").

31. *See infra* notes 61–67.

32. *See* RESTATEMENT (SECOND) OF TORTS § 652B (1977).

In 1890, Samuel Warren and Louis Brandeis called for the law to recognize a general right to privacy. They famously described privacy as the "right to be let alone."[33] But Warren and Brandeis's view of privacy was expansive—perhaps too expansive—protecting not just the right to be physically alone when desired, but the right to an "inviolate personality" from the "too enterprising press, the photographer, or the possessor of any other modern device for recording or reproducing scenes or sounds."[34] This more expansive view of privacy included a right to control the extent to which one's information was publicized, which raises First Amendment problems. But the core understanding of privacy as a right to be let alone is relatively uncontroversial.

Following the Warren and Brandeis Article, U.S. courts recognized a variety of privacy actions. In 1960, torts scholar William Prosser famously categorized some 300-plus suits arising from Warren and Brandeis's right to privacy as four torts: intrusion upon seclusion; public disclosure of private fact; false light; and appropriation.[35] Before Prosser's taxonomy, there was more variety in litigation but less national coverage; states recognized more causes of action, but fewer states recognized privacy torts.[36] Now nearly every state recognizes Prosser's four privacy torts.[37] But the spread of Prosser's torts also "fossilized" the development of U.S. privacy law, restricting the development of other related causes of action, like breach of confidence.[38]

Prosser's taxonomy has been much criticized. Some criticism arises from the tension between the disclosure torts and freedom of speech—a tension Prosser himself recognized.[39] Penalizing information distribution runs headlong into protection of free speech. Others criticize the Prosser taxonomy as failing to reach privacy problems of the information age.[40]

---

33. Warren & Brandeis, *supra* note 10, at 193.

34. *Id.* at 205–06.

35. William Prosser, *Privacy*, 48 CALIF. L. REV. 383, 389 (1960).

36. Neil M. Richards & Daniel J. Solove, *Prosser's Privacy Law: A Mixed Legacy*, 98 CALIF. L. REV. 1887, 1895, 1913 (2010) (pointing out that by the time of Prosser's Article, only a minority of states recognized privacy torts, but that the breadth of the understanding of privacy "germinated countless new torts to redress a variety of related yet distinct harms").

37. ROBERT M. O'NEIL, THE FIRST AMENDMENT AND CIVIL LIABILITY 77 (2001) (observing that every state but North Dakota and Wyoming recognizes the privacy torts in either statute or at common law).

38. Richards & Solove, *supra* note 36, at 1904 ("[W]hile Prosser gave tort privacy a legitimacy it had previously lacked, he also fossilized it and eliminated its capacity to change and develop.").

39. Neil M. Richards, *The Limits of Tort Privacy*, 9 J. TELECOMM. & HIGH TECH. L. 357, 365 (2011) (discussing the tension between disclosure torts and the First Amendment).

40. Danielle Keats Citron, *Mainstreaming Privacy Torts*, 98 CALIF. L. REV. 1805, 1810 (2010); Richards & Solove, *supra* note 36, at 1889.

The Prosser torts do, in practice, enforce a limited conception of privacy.[41] Courts have tended to rely on a privacy binary: information is either withdrawn and thus private, or available to others and thus public.[42] Once information is shared with others under this rubric, it can no longer be protected as private.

While some courts appear to recognize a more contextualized understanding of privacy—for example, a court found that a person's HIV status could still be considered private information even though it had been shared with more than sixty people[43]—that contextualized understanding often relies on the sensitivity of the type of information at issue. If information is health information, or related to the naked body, or otherwise falls into a category of information courts recognize as inherently sensitive, then sharing that information with other people or being in a public space does not necessarily make the information non-private in nature.[44]

The intrusion upon seclusion tort exemplifies the privacy binary: liability arises when individuals transgress into a private space.[45] It is possible for intrusion to take place in public, because "there may be some matters about the plaintiff, such as his underwear or lack of it, that are not exhibited to the public gaze."[46] But many courts afford no liability, for example, for an image captured on a public street.[47] Fourth Amendment jurisprudence until very recently echoed this reasoning: "A person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another."[48] While some courts have adopted a more nuanced view, until

---

41. Richards & Solove, *supra* note 36, at 1920 (observing that in applying the Prosser torts, "courts have relied upon antiquated and narrow understandings of privacy. . . . 'There can be no privacy in that which is already public'" (quoting Gill v. Hearst Publ'g Co., 253 P.2d 441 (Cal. 1953))).

42. *Id.* (noting that "privacy becomes an all-or-nothing affair, something that makes privacy virtually impossible in today's world where it is increasingly difficult (if not impossible) to keep much information completely hidden away").

43. Multimedia WMAZ, Inc. v. Kubach, 443 S.E.2d 491, 494 (Ga. Ct. App. 1994).

44. *See, e.g.*, Daily Times Democrat v. Graham, 162 So. 2d 474 (Ala. 1964) (protecting as private a woman's underwear when her skirt flew up at a funhouse ride).

45. RESTATEMENT (SECOND) OF TORTS § 652B cmt. c (1977) (explaining that liability arises only when individuals violate private space or private seclusion).

46. *Id.*

47. *See generally supra* note 30.

48. United States v. Knotts, 460 U.S. 276, 281 (1983); *see also* Florida v. Riley, 488 U.S. 445, 450–51 (1989) (finding no reasonable expectation of privacy where a greenhouse was visible by helicopter from navigable airspace 400 feet in the air); California v. Greenwood, 486 U.S. 35, 40–41 (1988) ("[H]aving deposited their garbage 'in an area particularly suited for public inspection

very recently, the Supreme Court has tended to address privacy through this binary framework.[49]

The historic tendency to view privacy and publicity in a binary framework runs broader than the application of the privacy torts. In both legal and political theory, the terms "private" and "public" often mark a dichotomy, rather than ends on a spectrum.[50] The private sphere is personal, intimate, even familial, while the public sphere usually involves civic participation and governance.

Within this binary, privacy can be, and often is, demarcated along physical lines. People withdraw to private spaces; hence U.S. privacy jurisprudence repeatedly recognizes the special nature of the home.[51] Or the private-public binary can instead focus on the kind of information at issue, requiring protection for intimate or sensitive information.[52] But neither understanding of privacy—as protecting privileged spaces, or protecting privileged information—accounts for protection of privacy in ordinary information incidentally revealed outside the home.

In fact, the revelation of ordinary information outside of the home is often used in both privacy jurisprudence and in philosophical debates as the easily dismissed pole of the privacy-publicity binary.[53] Even those

---

and, in a manner of speaking, public consumption, for the express purpose of having strangers take it,' respondents could have no reasonable expectation of privacy in the inculpatory items that they discarded." (citation omitted)); California v. Ciraolo, 476 U.S. 207, 215 (1986) (finding no reasonable expectation of privacy where marijuana plants were visible from 1000 feet in the air); United States v. Scott, 975 F.2d 927, 930 (1st Cir. 1992) ("[S]hredding garbage and placing it in the public domain subjects it to the same risks regarding privacy, as engaging in a private conversation in public where it is subject to the possibility that it may be overheard by other persons. Both are failed attempts at maintaining privacy whose failure can only be attributed to the conscious acceptance by the actor of obvious risk factors."). *But see* United States v. Jones, __ U.S. __, 132 S. Ct. 945, 945 (2012) (finding that the Fourth Amendment requires a warrant for applying a GPS tracker to a car).

49. *Id.* State constitutions have been found, by contrast, to protect privacy even in public spaces. *See, e.g.*, State v. Jackson, 150 Wash. 2d 251, 276–77, 76 P.3d 217, 231 (2003) (Washington State Supreme Court protecting against remote GPS tracking); State v. Boland, 115 Wash. 2d 571, 581, 800 P.2d 1112, 1117 (1990) (finding a valid privacy interest in trash).

50. Nissenbaum, *supra* note 5, at 584.

51. Florida v. Jardines, __ U.S. __, 133 S. Ct. 1409, 1419 (2013); Kyllo v. United States, 533 U.S. 27, 40 (2001); Desnick v. Am. Broad. Cos., 44 F.3d 1345, 1352–53 (7th Cir. 1995) (distinguishing *Dietemann v. Time, Inc.*, 449 F.2d 245 (9th Cir. 1971)); *see also* Warren & Brandeis, *supra* note 10, at 202 n.1 (noting that English courts held sacred the right to privacy within the home).

52. *See generally* Paul Ohm, *Sensitive Information*, 88 S. CAL. L. REV. (forthcoming 2015).

53. *See, e.g.*, Tom Gerety, *Redefining Privacy*, 12 HARV. C.R.-C.L. L. REV. 233, 271, 281 (1977) (defining privacy as an "island of personal autonomy" limited to the "intimacies of personal identity"); W.A. Parent, *Privacy, Morality, and the Law*, 12 PHIL. & PUB. AFF. 269, 271 (1983) (stating that all other information "cannot without glaring paradox be called private"). Nissenbaum calls this the "normative knock-down argument." Nissenbaum, *supra* note 5, at 575, 587.

advancing a more complex understanding of privacy will concede that privacy "does not assert a right never to be seen even on a crowded street."[54] That concession, however, has come under significant scrutiny recently, in both scholarship and jurisprudence.

B. Privacy in Public

Evolving technology has driven a parallel evolution in legal understandings of privacy in public.[55] The simple public phone booth forced the Supreme Court to re-evaluate its earlier conclusion that privacy would be protected only in the home. The Court instead delinked privacy protection from trespass, and devised its Fourth Amendment "reasonable expectation of privacy" test, also known as the *Katz* test.[56] Cellular telephones and their ability to cheaply and easily film and photograph activity in public have driven the enactment of voyeurism laws.[57] Now drones and their ability to achieve perspectives once attainable only by aircraft or crane have driven states to enactment drone privacy laws.[58]

Scholars have proposed competing theories of privacy to push back against the binary conceptualization of information as either completely withdrawn, or completely available. Often, these competing conceptualizations have been used to address the question of privacy in public.

There is considerable support for why information revealed in public should be protected from government surveillance. Extensive surveillance can produce both conformity and anxiety.[59] When the government wields public surveillance as a tool, this shifts the balance of power between citizens and government, and makes citizens less able to effect democratic change.[60] Under a variety of constitutional justifications—stemming from both the Fourth Amendment and the First Amendment—it can be argued that ordinary activities performed in

---

54. Jeffrey H. Reiman, *Privacy, Intimacy, and Personhood*, 6 PHIL. & PUB. AFF. 26, 44 (1976).

55. *See, e.g.*, Nissenbaum, *supra* note 5, at 576.

56. Olmstead v. United States, 277 U.S. 438 (1928), *overruled by* Katz v. United States, 389 U.S. 347 (1967).

57. *See, e.g.*, 18 U.S.C. § 1801 (2012).

58. Margot E. Kaminski, *Drone Federalism: Civilian Drones and the Things They Carry*, 4 CALIF. L. REV. CIRCUIT 57, 57–59 (2013); Calo, *supra* note 22.

59. Margot E. Kaminski & Shane Witnov, *The Conforming Effect: First Amendment Implications of Surveillance, Beyond Chilling Speech*, 49 U. RICH. L. REV. 465, 483–93 (2014).

60. *Id.*; *see also* Christopher Slobogin, *Public Privacy: Camera Surveillance of Public Places and the Right to Anonymity*, 72 MISS. L.J. 213, 237–52 (2002).

public should be protected from government surveillance.[61]

However, when private citizens conduct surveillance on other private citizens, the question of privacy harm becomes more complicated. Surveillance by private actors poses the challenge of balancing individual rights.[62] A subject's right to be free from surveillance comes into conflict with the right of the observer to gather information, or to merely observe and remember.[63] A more precise explanation of public privacy harms is necessary; one capable of distinguishing between different degrees of harm.

One way to understand privacy harms involving information gathered in public is to look to harms associated with data use—that is, private-sector data-mining. Writing about privacy in public, Helen Nissenbaum explained that "people have a robust sense of the information about them that is relevant, appropriate, or proper to particular circumstances, situations, or relationships."[64] They choose to reveal information under particular circumstances, expecting that it will not travel beyond those settings.

The privacy harm occurs when information is decontextualized, and moved into another setting despite norms suggesting it will not be moved. Nissenbaum argued that this theory of what she terms "contextual integrity" is critical to understanding why we should protect privacy in public.[65] Nissenbaum explains that privacy, understood as contextual integrity, is crucial to the ability to "define the nature and degree of closeness of relationships," which in turn is "an important aspect of personal autonomy."[66]

Nissenbaum's characterization of information privacy as contextual integrity has been a particularly influential alternative to the privacy

---

61. Slobogin, *supra* note 60, at 252–72. *See generally* David Gray & Danielle Keats Citron, *A Shattered Looking Glass: The Pitfalls and Potential of the Mosaic Theory of Fourth Amendment Privacy*, 14 N.C. J.L. & TECH. 381 (2013); Margot E. Kaminski, *Real Masks and Real Name Policies: Applying Anti-Mask Case Law to Anonymous Online Speech*, 23 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 815 (2013); Orin Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801 (2004).

62. Kaminski, *supra* note 58, at 62–63; Nissenbaum, *supra* note 5, at 571 ("[P]rotecting privacy for one person inevitably leads to restraints on the freedom of another or others, or may even result in harms to them.").

63. Seth F. Kreimer, *Pervasive Image Capture and the First Amendment: Memory, Discourse, and the Right to Record*, 159 U. PA. L. REV. 335, 337 (2011). *See generally* Bambauer, *supra* note 4.

64. Nissenbaum, *supra* note 5, at 581.

65. *Id.* at 21.

66. *Id.* at 22.

binary.[67] The theory of contextual integrity currently plays a crucial role in policy conversations about big data and privacy; the May 2014 White House Report on Big Data refers to the idea of a "no surprises" rule for data use.[68] Data should not be used out of context in a way that would surprise the data subject. And there are portions of U.S. jurisprudence that support contextual integrity as an applied theory.[69]

But a theory of privacy as contextual integrity focuses on the processing of data rather than the gathering of it. Contextual integrity emphasizes concerns over shifting information from one context to another, and collating information to reveal patterns.[70] Surveillance in public is problematic under this rubric because it enables both decontextualization and collation; but surveillance by itself is not necessarily problematic in the absence of data use. Contextual integrity thus poses a strong argument for why information revealed in public should not be moved or manipulated, but only secondarily explains why it should not be gathered in the first place.

When it comes to evaluating existing surveillance laws, contextual integrity is not descriptively accurate, and struggles as a guide for legislators. Descriptively, many of the laws governing private information gathering do not address either decontextualization or collation; they often don't discuss data use or misuse.[71] They focus instead on the moment of information collection itself. As a guide for new legislation, contextual integrity is challenging. Legislators would have to either delegate heavily to courts to determine when a "surprise" about data use is problematic, or would have to devise laws that are tailored to or responsive to information norms varying across a vast multitude of social situations. For example, let's say that an individual

---

67. NISSENBAUM, *supra* note 1, at 2–3 (2010).

68. *See, e.g.*, EXEC. OFFICE OF THE PRESIDENT, BIG DATA: SEIZING OPPORTUNITIES, PRESERVING VALUES 56 (2014), *available at* https://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf; Alexis C. Madrigal, *The Philosopher Whose Fingerprints Are All Over the FTC's New Approach to Privacy*, THE ATLANTIC (Mar. 29, 2012), http://www.theatlantic.com/technology/archive/2012/03/the-philosopher-whose-fingerprints-are-all-over-the-ftcs-new-approach-to-privacy/254365/.

69. *See, e.g.*, Watchtower Bible & Tract Soc'y of N.Y., Inc. v. Village of Stratton, 536 U.S. 150, 165–66 (2002). *See generally* Andrew D. Selbst, *Contextual Expectations of Privacy*, 35 CARDOZO L. REV. 643 (2013).

70. Nissenbaum, *supra* note 5, at 19.

71. *See, e.g.*, GA. CODE ANN. § 16-11-61(b) (West, Westlaw through 2015 Reg. Sess.) (defining "peeping Tom" as one "who peeps through windows or doors, or other like places . . . for the purpose of spying upon or invading the privacy of the persons spied upon and the doing of any other acts of a similar nature which invade the privacy of such persons"); RESTATEMENT (SECOND) OF TORTS § 652B (1977).

has his picture taken while walking into a pet store on a relatively quiet street. Does it violate contextual integrity for that information to be sent to PETA? To his mother? To an advertiser for pet goods? It is hard to determine at what point the reuse or distribution of a piece of information becomes problematic, and with respect to whom.

Joel Reidenberg recently revisited this problem of privacy in public, arguing for a theoretical shift from a binary conception of privacy to demarcation along "governance-related" and "non-governance related" lines.[72] Observing how ill-equipped the "reasonable expectation of privacy" approach is for dealing with problems of the information age, Reidenberg proposes what he deems a variation on Nissenbaum's theory.[73] He suggests that courts should apply a "public significance filter" to determine whether information is private or not; if it is about governance, it is not private, and if it is not about governance, it is private.[74] Reidenberg explains that this filter will preserve journalistic uses of important information and thus poses no First Amendment concerns.[75]

Distinctions between private and newsworthy information, or information of "public concern," abound in privacy law.[76] Reidenberg's suggested filter thus has the benefit of resonating with both recent historical examples and some case law. However, it fails to provide a workable theory of privacy for prohibitions on information gathering for three reasons. First, like Nissenbaum's theory of contextual integrity, the private-unless-newsworthy framework does not reflect how legislators have actually been drafting surveillance laws. Most surveillance laws protect as private a segment of information narrower than all-information-that-is-not-newsworthy. Second, the idea of protecting information as private unless it has a nexus with governance has been rejected by a number of courts concerned with restricting newsgathering, or freedom of expression more generally.[77] And third, it is often difficult to distinguish between high-value, newsworthy information and private information.[78] To be fair, the Supreme Court has occasionally hinted that

72. *See generally* Joel R. Reidenberg, *Privacy in Public*, 69 U. MIAMI L. REV. 141 (2014).

73. *Id.* at 155.

74. *Id.*

75. *Id.* at 158.

76. For example, there is a newsworthiness exception to the tort of public disclosure of private fact. *See, e.g.*, Sipple v. Chronicle Publ'g Co., 201 Cal. Rptr. 665, 669–70 (Ct. App. 1984); Shulman v. Grp. W Prods., 955 P.2d 469, 479 (Cal. 1998).

77. *See, e.g.*, Gill v. Hearst Pub. Co., 253 P.2d 441, 445 (Cal. 1953).

78. *See* Bambauer, *supra* note 4, at 97–100 (discussing the importance of types of information

distinctions between newsworthy and private information may matter,[79] but the Court's First Amendment jurisprudence in general is wary of distinctions between high and low value speech.[80] Requiring courts to assess just how newsworthy information is leads into an age-old conflict between privacy and the First Amendment—and it is not clear that surveillance laws need embody that conflict, or at least be placed so squarely in its crosshairs.

C. The Need for a New Approach

We need a new way to understand the government interest in surveillance laws, but that approach need not throw out everything useful about older frameworks. While the privacy binary is unworkable when it comes to discussing privacy in public, the understanding of privacy as seclusion or withdrawal has the benefit of resonating with fundamental intuitions, derived from social experience. The home is special from a privacy perspective; other private spaces can be special, too. Using withdrawal tactics, whether by hiding behind walls or keeping information within a close circle of friends, indicates that an individual believes information is more private.[81] Useful and longstanding intuitions about privacy should not be abandoned simply because they have given rise to reductionist understandings of when information is private. Rather than departing from the strength of the seclusion model, we should ask how seclusion relates to attempts to protect privacy in non-secluded spaces. Identifying what was valuable in past privacy intuitions is particularly important as boundaries between home and not-home, and the physical and online world, become fuzzier and more fluid in light of technological and social change.

Private surveillance laws are similar to each other, not solely because they focus on the moment at which information is collected. They operationalize the same government interest, albeit of different degrees of strength. This Article argues that the government interest in private

---

beyond newsworthy information).

79. *See, e.g.*, Bartnicki v. Vopper, 532 U.S. 514, 525 (2001).

80. United States v. Stevens, 559 U.S. 460, 470 (2010) ("The First Amendment's guarantee of free speech does not extend only to categories of speech that survive an ad hoc balancing of relative social costs and benefits. The First Amendment itself reflects a judgment by the American people that the benefits of its restrictions on the Government outweigh the costs."). *Contra Shulman*, 955 P.2d at 479 ("We therefore agree with defendants that under California common law the dissemination of truthful, newsworthy material is not actionable as a publication of private facts.").

81. For a discussion of such withdrawal tactics in the digital space, see Hartzog & Stutzman, *supra* note 1, at 14.

surveillance laws is an interest in enabling individuals to engage in boundary management at the moment or moments information gathering occurs. Thus, the government has an interest not just in preventing the reuse or distribution of data; it has an interest in limiting and sometimes preventing data collection.

III. PRIVACY AS BOUNDARY MANAGEMENT

Laws that prohibit private surveillance protect the government's interest in enabling individuals to engage in boundary management in physical space, including by using the physical features of that space. These laws are sensitive to the contexts created in and using the physical environment. The state interest in enabling boundary management exists in both private and public spaces. The similarity between these laws shows that legislators do understand privacy as existing on a continuum, not a binary: The government interest in protecting individuals in public is the same kind of interest invoked in protecting privacy in private spaces.

These laws do not identify a particular type of information as private information. Instead, they enable individuals to negotiate relationships with other people—including strangers—by relying on known features of their environment. Sometimes a law enables effective relationship navigation by requiring notice of surveillance, which enables an individual to adapt her behavior (at least in theory, since in practice behavior often cannot be adapted due to economic or social necessity). Sometimes a law enables boundary management by preserving an environment or context as free from recording. These laws thus can appear at first glance conservative—some, after all, are aimed at keeping things the way they were before the introduction of new surveillance technology. But the government interest is not just in abstract conservation: It is in preventing concrete shifts in behavior resulting from changes to the environment.

The framing of privacy as boundary management has been addressed elsewhere in the legal literature, but it has not been applied where it naturally fits: to identify the government interest in surveillance laws governing interactions between private actors in physical, rather than online, space. Boundary management has been referenced in the legal literature in the online context,[82] and to provide a general definition of

82. Paul Dourish & Leysia Palen, *Unpacking "Privacy" for a Networked World*, *in* PROCEEDINGS OF THE ACM CHI 2003 HUMAN FACTORS IN COMPUTING SYSTEMS CONFERENCE 129 (2003); Hartzog & Stutzman, *supra* note 1.

privacy.[83] It has not been applied at any length, however, to existing real-world surveillance laws.

A. The Boundary Management Framework

Boundary management is a concept developed by social psychologist Irwin Altman in the 1970s.[84] Altman worked in the field of environment and behavior studies (now known as environment-behavior studies), which considers the connection between environmental design and psychological development. Altman's conceptualization of privacy emerged from studies of crowding, personal space, territoriality, and other human behavior that uses or responds to features of the physical environment in the regulation of social relationships.[85]

Altman observed that people interact with others within their environment as part of an optimizing process.[86] People attempt to maintain "an optimal degree of desired access of the self to others at any moment in time."[87] This optimizing process is what Altman terms privacy. It is not static nor binary, but dynamic and dialectic.[88] Altman's idea of privacy is the dynamic regulation of exposure along a "range of openness-closedness of the person or group," shifting over time and circumstances.[89] In other words, people dynamically navigate actions and interactions with an ideal of disclosure to others in mind.

Boundary management can be a useful framework for discussing information privacy.[90] However, Altman's observations are particularly helpful for understanding privacy governance in the physical world. The

---

83. Julie Cohen employs Altman's theory as the foundation of her definition of privacy. *See* Julie E. Cohen, *What Privacy Is For*, 126 HARV. L. REV. 1904, 1927 (2013) [hereinafter Cohen, *What Privacy Is For*] ("[P]rivacy in the dynamic sense is 'an interest in breathing room to engage in socially situated processes of boundary management.'" (quoting the definition developed in her book, JULIE E. COHEN, CONFIGURING THE NETWORKED SELF: LAW, CODE, AND THE PLAY OF EVERYDAY PRACTICE 16–20, 107–26, 149 (2012) [hereinafter COHEN, CONFIGURING THE NETWORKED SELF])).

84. *See generally* ALTMAN, *supra* note 6.

85. *Id.*

86. *Id.* at 11.

87. *Id.*

88. Dourish & Palen, *supra* note 82, at 1 (describing Altman's "model of privacy as a dynamic, dialectic process").

89. Nathan Witte, *Privacy: Architecture in Support of Privacy Regulation* (May 16, 2003), https://etd.ohiolink.edu/!etd.send_file?accession=ucin1053701814&disposition=inline.

90. COHEN, CONFIGURING THE NETWORKED SELF, *supra* note 83, at 149; Dourish & Palen, *supra* note 82; Woodrow Hartzog & Fred Stutzman, *Boundary Regulation in Social Media*, *in* PROCEEDINGS OF THE ACM 2012 CONFERENCE ON COMPUTER SUPPORTED COOPERATIVE WORK 769 (2012), *available at* http://fredstutzman.com/papers/CSCW2012_Stutzman.pdf.

concept of boundary management stems from observations about how people interact in—and use features of—physical space. Because of its connection to the physical environment, Altman's theory best explains the government's interest in a variety of laws governing information capture in the physical world.[91]

According to Altman, people use a wide variety of strategies and mechanisms to achieve the optimal degree of access at a given moment. These strategies or mechanisms include verbal behavior, paraverbal behavior (such as tone of voice), nonverbal behavior (such as movements), personal space, territory (including the use of objects in a particular locale), and cultural mechanisms.[92] Boundary management mechanisms include the use of environmental artifacts like doors and walls. If you want to be secluded, you hide behind a wall. If you want to be open to one person, but not to everyone else, you have your conversation with that one person very quietly, or within closed walls that exclude everybody else. But boundary management mechanisms also include decisions about the duration of the interaction (time), the depth of the interaction (how much you say), the truthfulness of the interaction (whether you lie), and the use of nonverbal cues (refusing to make eye contact) or cultural tropes (using an expression or making a joke) to indicate withdrawal or engagement. All of these mechanisms are used to regulate how much of the self is accessible to other people in a given interaction.

Removing physical boundaries does not make people abstain from boundary management. Instead, removing physical boundaries often results in people changing their use of behavioral mechanisms. If you take away a wall, people may employ other forms of cover or withdrawal, such as wearing more clothing,[93] saying less, or engaging in culturally taught mechanisms of withdrawal. Taking away one mechanism (the wall) can cause an individual to use another (lying).

Altman observed this relationship between boundary management mechanisms across cultures. People across different cultures still try to optimize their social accessibility, but "what differs among cultures is the particular configuration of mechanisms the people use."[94] Thus even

---

91. It can also explain how people behave in networked or digital spaces, but there the mechanisms are often metaphors, and genres of boundary management are arguably less well-established.

92. ALTMAN, *supra* note 6, at 11.

93. *Id.* at 36–37 (people use clothing to "tell the world who they are, to help define situations, and to reflect their status roles. . . . People also use clothing to signal their approachability").

94. Irwin Altman, *A Personal Perspective on the Environment and Behavior Field*, *in* VISIONS OF

cultures that at first glance appear not to value privacy in the binary sense of full withdrawal will use other "behavioral mechanisms for managing the social accessibility of people to one another."[95] Individuals in a culture that does not generally prioritize private rooms may instead navigate boundary management by being more socially withdrawn at home.

A crucial feature of boundary management is that it takes place across the dimension of time. Regulating the accessibility of the self to others is not a one-time decision. It entails calculations concerning duration, repetition, and frequency of exposure. It also often entails relying on the ephemeral nature of interactions, and the imperfection of human memory.[96]

Effective boundary management depends not only on observed features of humans in general, but on knowledge of one's relationship with a particular person. People tend to increase self-disclosure where a person reciprocates, unless they expect nonreciprocal behavior because that person fills a particular social role (e.g., of teacher, priest, therapist).[97] Self-disclosure tends to be at its highest early on in a relationship.[98] People also tend to increase self-disclosure when they trust somebody not to reveal that information to a third party. Respect of the "dyadic boundary"—"the boundary within which it is safe to disclose to the invited recipient and across which the self-disclosure will not pass"—may increase disclosure.[99] Thus, perceptions of the person to whom one is disclosing information—their trustworthiness or social role—can affect the extent of a person's optimal level of openness towards that person.

Boundary management is highly dependent on context, but this does not mean that people always take the time to figure out the precise nature of the context of an interaction. People use shortcuts. They often resort to familiar patterns of behavior, based on learned assumptions about their environment. Scholars have called these patterns "genres of

---

AESTHETICS, THE ENVIRONMENT & DEVELOPMENT 118 (Roger M. Downs et al. eds., 1991); *see also* ALTMAN, *supra* note 6, at 12–17.

95. ALTMAN, *supra* note 6, at 12.

96. Dourish & Palen, *supra* note 82, at 2 (noting that "the recordability and subsequent persistence of information, especially that which was once ephemeral, means that audiences can exist not only in the present, but in the future as well").

97. VALERIAN J. DERLEGA & ALAN L. CHAIKIN, SHARING INTIMACY: WHAT WE REVEAL TO OTHERS AND WHY 108 (1975).

98. Valerian Derlega & Alan Chaikin, *Privacy and Self-Disclosure in Social Relationships*, 33 J. SOC. ISSUES 102, 102–15 (1977).

99. *Id.* at 104.

disclosure."[100] Genres in this context are the "regularly reproduced arrangements of people, technology and practice that yield identifiable and socially meaningful styles of interaction."[101] People learn to resort to a particular genre of disclosure, depending on past practice and on cues given by their environment. A person might act a particular way in the classroom, another way on a public street, and yet another way in a public but secluded park. That person might use social and physical cues to resort to a park genre of behavior, a school genre of behavior, and so forth.

Genres of disclosure evolve as technology and social practices change.[102] For example, where once people might have assumed that an action in the London streets would not be recorded, now they may be aware of the prevalence of CCTV cameras, and act accordingly. Instead of acting within the old genre of public street behavior that was appropriate when there were no cameras, they may now act as though other people are watching. There can be a significant government interest in either preserving certain genres of disclosure, or in alerting people so that they do not inaccurately rely on a past genre once circumstances have changed.

B. The Government's Interest in Boundary Management

Altman's theory of privacy as boundary management is a strong foundation for understanding the government interest or interests behind private surveillance laws. This section builds on Altman's theory of privacy as boundary management to identify the government's interest in enacting surveillance laws. The government interest implicated by framing privacy as boundary management is twofold. First, the government may have an interest in preventing people from miscalculating their boundaries. Second, the government may have an interest in preserving a particular genre of boundary management—not out of nostalgia or fear of technological change, but because of the problems that might occur if one forces people to shift boundary management tactics.

---

100. Dourish & Palen, *supra* note 82, at 5.

101. *Id.*

102. *Id.*

1. *Allowing an Individual to Calculate Her Desired Degree of Disclosure*

The government has an interest in preventing people from miscalculating their degree of disclosure. This interest is implicated when a person has a desired degree of openness to the world, but miscalculates her use of management mechanisms based on settled expectations about her environment. For example, a person might do a silly dance in her office every morning before sitting down to answer emails, relying on boundary management mechanisms such as walls and having an office on the fourth floor to prevent other people from seeing her. But if a drone is able to capture that silly dance through the fourth story window, then the person may want to change her calculation of socially optimal behavior based on new understandings of her environment.

As our environments change around us, due to developments in both technology and social practice, the government may have a strong interest in alerting us to those changes by requiring notice. Requiring notice allows the surveillance subject to recalculate her mechanisms for maintaining an optimized balance of openness and closedness in a given environment. Notice and consent are thus an important aspect of many information capture statutes. Notice can also trigger social enforcement through shaming of the person conducting surveillance. An unobserved observer may be less subject to the pull of social norms, but an announced observer can be subjected to shaming.

2. *Preventing Undesirable Behavioral Changes*

The government can also have an interest in preserving a particular genre of boundary management. Recall that people often resort to shortcuts based on past experiences, triggered by environmental cues. When shortcuts invoke site-specific or person-specific patterns, they can be described as genres of boundary management (e.g., behaving different ways in public, at the mall, in church, in one's home, at one's office).[103] The government can have an interest in preserving a genre of behavior, not because the genre itself is particularly valuable (although it can be), but because the alternative could have significant consequences. Altman observed that people substitute mechanisms to maintain an ideal

---

103. *See* ERVING GOFFMAN, THE PRESENTATION OF SELF IN EVERYDAY LIFE (1959). Another way to understand Goffman's masks is as genres of boundary management, directed at different audiences and triggered by both environmental cues and the nature of one's understood audience.

level of openness or closedness. If a person lacks a wall, they may change their verbal, paraverbal, or nonverbal behavior instead. The silly dancer of the earlier example may modify her behavior—that is, stop dancing—to maintain the same level of openness-closedness, and there may be costs attributable to that behavioral change. Silly dancing might be necessary for productivity, or have an expressive value, or form part of that person's definition of herself. For any of these reasons, the government may have an interest in preserving a genre of boundary management, and preventing the surveillance subject from shifting behavior to reach the same level of optimization.

Take the example of laws prohibiting up-skirt photography, discussed more fully in Part V.A.1 below. The government interest in prohibiting up-skirt photography in public places is not limited to the protection of a particular type of private information (that is, what's under the skirt), or an interest in protecting the dignitary interests of the observed. It is also an interest in genre preservation. In pluralistic American society, we envision public spaces as a place where people can wear many different types of clothing. Permitting surreptitious up-skirt photography likely will not cause women to recalibrate their optimal degree of nudity in public. More likely, it will cause a shift in the boundary management mechanisms deployed, and more women will stop wearing skirts and wear more conservative coverings instead. The government has a legitimate interest in preventing that behavioral shift, thus preserving a pluralistic public space.[104]

The government interest in preventing an undesirable shift in behavior can be particularly important when it comes to speech concerns. The government may have an interest in enacting laws to guard a trustworthy relationship or conversation. Protection of this sort can encourage disclosure within that conversation, and avoid a resulting chill in speech.[105]

The government's interest in bolstering or reinstating older mechanisms for boundary management is thus not based solely on nostalgia. The government interest can be articulated as a desire to prevent shifts to different kinds of boundary management mechanisms. If Altman is correct that in the absence of physical mechanisms, people optimize their social accessibility through decisions to speak or not

104. It also can have a legitimate interest in protecting the individual from dignitary harms and an inability to self-define through clothing. These are related but not identical to the boundary management interest.

105. DERLEGA & CHAIKIN, *supra* note 97.

speak, to repress, or to more closely follow cultural patterns,[106] then the government may be interested in preventing those kinds of behavioral shifts in certain contexts.

Scholars have observed that law often steps in where new technologies disrupt the environment in which behavior takes place. Orin Kerr recently noted, for example, that new technologies can disrupt the balance of power between individuals and the government by lowering costs of surveillance.[107] Courts adjust Fourth Amendment doctrine in light of new technologies to preserve the status quo balance of power. Harry Surden has similarly written about the need to recognize implicit "structural rights" to privacy: rights that are structurally provided by the physical environment and erased by new technologies.[108] An example of a "structural right" would be the existence of a physical wall. When technology enables individuals to look through a wall, then law can step in to provide a legal barrier where formerly there was a structural, environmental barrier.

But both of these views focus on law as a constraint, whether on law enforcement or on private actors. They emphasize the government's interest in replacing physical environmental restrictions with legal ones. In Surden's case, this builds on Lawrence Lessig's conception of governance as including norms, architecture, the market, and the law.[109] Where physical architecture changes, the reasoning goes, law might step in to achieve the same constraints on behavior.

Framing privacy as boundary management shifts the focus. Instead of asking whether there is a government interest in maintaining a particular status quo level of constraints on the observer's actions, the focus instead is on the value of the law to the observed. The government interest is not just in technophobically preserving a particular environmental balance; it is in enabling observed individuals to rely on and use features of their environment in self-developing ways.

Recharacterizing the government interest in private surveillance laws should help courts shift away from examining whether the information at issue is adequately private within the private-public binary. Instead, courts can understand privacy laws as empowering individuals to modify their behavior, or protecting individuals from having to modify their behavior at all. It shifts the focus from assessing whether a particular

106. ALTMAN, *supra* note 6, at 12.

107. Orin S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 HARV. L. REV. 476, 478 (2011).

108. Harry Surden, *Structural Rights in Privacy*, 60 SMU L. REV. 101, 101 (2007).

109. *Id.* at 103.

piece of information is inherently sensitive to looking to the impact of technological changes on individual autonomy and behavior.

These government interests will not, and should not, always be considered adequate. But it is important that courts understand that government interests go beyond preserving privacy in secluded spaces, or preserving privacy in sensitive information. The interest in protecting boundary management is an interest in enabling self-development and preventing cultural shifts that will occur if the law does not step in.

The underlying value of boundary management thus is tied to how one conceives of and values the individual self in society. Boundary management sits naturally with the liberal idea of the autonomous self, which should not be unduly restricted from making choices. But boundary management can also sit comfortably with a more complicated idea of a non-liberal self.[110] The non-liberal self is not isolated or stable like the liberal self, but is in constant development, influenced by and influencing other people and society.[111] One value of the boundary management framework is that it can be used with either conception of the self, liberal or not, which lets it both fit within dominant legal and political theory, and rest comfortably with criticisms of that theory.

C. *Enabling Boundary Management Protects Important Social Values*

Protecting individuals' ability to boundary-manage can protect important social values. Enabling boundary management respects individual autonomy. It allows for the formation of valuable relationships by enabling trust. It prevents conformity, which is valuable for purposes of self-governance.[112] It allows for the formation of both individual and community identities.[113] It prevents chilling effects, power imbalances, vulnerability harms, and relationship harms.[114] In short, the values implicated by protecting or enabling boundary management are compelling. Governments may enact these laws from a wide variety of philosophical perspectives; and protecting individuals from boundary management harms can be understood to serve a wide

110. Cohen, *What Privacy Is For*, *supra* note 83, at 1905 ("[T]he liberal self who is the subject of privacy theory and privacy policymaking does not exist . . . . [T]he self who is the real subject of privacy law and policy is socially constructed . . . .").

111. *Id.* at 1906.

112. Kaminski & Witnov, *supra* note 59.

113. Robert C. Post, *The Social Foundations of Privacy: Community and Self in the Common Law Tort*, 77 CALIF. L. REV. 957, 957–59 (1989).

114. SOLOVE, *supra* note 26, at 174–79 (listing these harms and more).

variety of values.

IV. POTENTIAL CRITICISMS OF BOUNDARY MANAGEMENT

The most significant criticism of boundary management is that it can evince a bias against technological change. When legislators enact laws to preserve particular genres of boundary management, this argument goes, they are refusing to let society evolve. It can be hard to distinguish between Luddites who unreasonably and vaguely fear new technologies, and people who want to protect genuine privacy interests. As Nissenbaum has noted, "critics may argue that it is simply a matter of time before people will become accustomed to the new order brought about by information technology and readily accept the new privacy conventions of public surveillance."[115]

The boundary management framework is explicitly not, however, about preserving the status quo for preservation's sake. It requires legislators to consider *why* they want to preserve a particular genre of boundary management around certain information or in a particular location or against a particular technology. It focuses on real concerns that individuals will shift their behavior in the absence of legal intervention. It may be that some behavioral shifts are not worth preventing. But it is abundantly clear that behavioral shifts do occur as a result of surveillance, and that some carry real harms to a pluralistic democratic society.[116] A legislature can have a legitimate interest in preventing those shifts.

Requiring notice can be a less restrictive way to address boundary management interests rather than prohibiting recording entirely. Prohibiting surreptitious recording effectively requires notice by making surveillance legal only when the recorder notifies her subject.

Surveillance laws built on a boundary management framework are in fact less conservative than banning surveillance involving, say, a particular type of information. Boundary management laws shift the cultural decision about a desirable level of privacy from the legislature to the individual who is being observed. The laws centering on notice let individuals calibrate an ideal level of disclosure, rather than relying on the legislature to identify a "sensitive" category of information. Such laws allow for more flexibility for normative change over time.

A different line of criticism stems from the healthy skepticism privacy scholars have for reliance on self-management in the privacy context.

---

115. Nissenbaum, *supra* note 5, at 583.

116. *See, e.g.*, Kaminski & Witnov, *supra* note 59.

Giving notice and control to individuals often does not work because of market failures, individuals' misplaced optimism, and inherent misunderstandings about big data.[117] However, prohibitions on surveillance need not take the place of data privacy regimes aimed at protecting even those individuals who have failed to accurately calibrate their privacy preferences at the moment information is gathered. The two types of laws—surveillance laws and data regulation—are complimentary, not substitutes.

V. BENEFITS OF THE BOUNDARY MANAGEMENT FRAMEWORK

The government's interest in preventing private surveillance is an interest in enabling or preserving boundary management by the individual being observed. This understanding of the privacy interest at stake has four benefits: First, it descriptively maps onto existing surveillance laws. Second, it allows courts to more clearly articulate the government interest at stake in these laws, instead of just referring vaguely to privacy. Third, it shows that private surveillance laws can protect First Amendment interests, rather than just be in conflict with them. Boundary management suggests that people disclose more when they trust that information will not travel; and in fact, several courts appear to understand this. Fourth, the boundary management framework will enable legislators to more thoughtfully enact new surveillance laws, governing new technologies.

A. Descriptive Accuracy

The boundary management framework is descriptively accurate: Legislators have in fact enacted a range of laws that enable individuals to dynamically manage their desired degree of disclosure by using or relying on features of their environments.

The oldest examples of these laws are relatively well-known and perhaps the most intuitive. They address the breach of physical barriers

---

117. *See, e.g.*, Paul M. Schwartz, *Beyond Lessig's* Code *for Internet Privacy: Cyberspace Filters, Privacy-Control, and Fair Information Practices*, 2000 WIS. L. REV 743; Daniel J. Solove, *Introduction: Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1880, 1880 (2013) ("Privacy self-management takes refuge in consent. It attempts to be neutral about substance . . . and instead focuses on whether people consent to various privacy practices. Consent legitimizes nearly any form of collection, use, or disclosure of personal data. Although privacy self-management is certainly a laudable and necessary component of any regulatory regime, I contend that it is being tasked with doing work beyond its capabilities.").

such as walls, either through physical trespass or by looking or listening through an aperture such as a window. These laws could be overlooked as irrelevant to conversations about privacy in public, because functionally they protect private spaces. That would be a mistake. These laws do not merely protect a particular location; they bolster physical barriers with legal barriers, so that individuals can rely on walls to prevent disclosure. This is the same function that other surveillance laws serve, just in different contexts and spaces, and with other boundary-management mechanisms.

A second type of boundary management law addresses technologies that use sense-enhancement or an unusual perspective to create, not physical, but constructive holes in the wall.[118] Instead of focusing on a physical barrier, these laws target technologies that alter the object of surveillance's degree of expected disclosure without providing notice. These are also boundary management laws. They provide legal protection to ensure that a person accurately calculates her degree of disclosure in light of the presence of technologies that unexpectedly widen the potential audience for her behavior.

A third type of surveillance law also addresses the use of technology instead of the physical breach of physical walls. But instead of focusing on the use of technology to enter into a private sphere unnoticed or from afar, these laws focus on the use of technology to alter the ephemerality of interactions. These laws target recording. Laws that target recording are a type of boundary management law, because ephemerality is a feature of the environment that individuals rely on when calculating their ideal degree of disclosure. Impermanence over time is, in other words, a barrier people rely on in social interactions in the real world. When recording technologies make interactions more permanent, an individual's calculation of optimal disclosure within an interaction and over time will change.

1. Private Spaces and Physical Barriers

Earlier privacy laws address the breach of physical barriers through physical or sensory entrance into a physical space. These laws preserve a person's ability to rely on walls or clothing as barriers against unwanted

118. I draw on California's paparazzi law in distinguishing between physical and constructive invasions of privacy. *See* CAL. CIV. CODE § 1708.8(a)–(b) (West, Westlaw through 2015 Reg. Sess.) ("A person is liable for physical invasion of privacy when the defendant knowingly enters onto the land of another person without permission .... A person is liable for constructive invasion of privacy when the defendant attempts to capture [recordings or images] ... through the use of any device, regardless of whether there is a physical trespass ....").

observers. They prevent nosy intruders from taking advantage of unobserved apertures, such as windows.

One of the earliest boundary management laws, eavesdropping, was a nuisance at common law. William Blackstone defined eavesdropping as a combination of information gathering and dissemination.[119] To eavesdrop, as Blackstone defined it, was to "listen under walls or windows, or the eaves of a house, to hearken after discourse, and thereupon to frame slanderous and mischievous tales."[120] The information-gathering portion of the eavesdropping offense clearly goes to boundary management. Banning listening in through walls, windows, or eaves provides legal reinforcement to the physical barriers of a house. The law stepped in to supplement physical boundaries, and to enable people within the home to trust that their walls, windows, and eaves effectively bordered a safe space for disclosure. The offense of eavesdropping is thus, at its heart, about boundary management, and goes to preserving the genre of actions and interactions in the home.

The tort of intrusion upon seclusion, like eavesdropping, often governs boundary management in a physical space. The tort entails an intentional intrusion that is highly offensive to a reasonable person.[121] Although intrusion upon seclusion does not identify particular boundaries or particular technological means of transgressing them, the tort centers on the law stepping in to reinforce a physical or normative boundary that has been transgressed.

Intrusion upon seclusion does not necessarily govern a specific space, barrier, or technology. In practice, however, courts have often limited the tort of intrusion upon seclusion to protecting a private space—a space where there is a reasonable expectation of privacy or seclusion. Many courts afford no liability, for example, for image capture on a public street.[122] However, the Restatement definition of the tort notes that there are some matters, even in public, that have not been submitted to the public gaze and therefore may be private.[123]

Peeping Tom laws demonstrate a narrower form of boundary management governance. In Peeping Tom laws, the state legislature,

---

119. 4 WILLIAM BLACKSTONE, COMMENTARIES *169.

120. *Id.*

121. RESTATEMENT (SECOND) OF TORTS § 652B (1977).

122. *Id.* at cmt. c (explaining that liability arises only when individuals violate private space or private seclusion).

123. *Id.* ("Even in a public place, however, there may be some matters about the plaintiff, such as his underwear or lack of it, that are not exhibited to the public gaze, and there may still be invasion of privacy when there is intrusion upon these matters.").

rather than courts, identifies the boundary that cannot be transgressed. This makes the laws more specific and less flexible. A number of Peeping Tom laws define the offense as peering through windows, doors, or other apertures.[124] Commenters explain that these statutes can be of limited practical value because they require catching the Peeping Tom spying at the aperture.[125] Several states require trespass in addition to the act of peeping, further limiting the scope of the laws.[126]

A third category of peeping laws defines the offense not by the aperture through which the offender looks, but by the secrecy of the spying.[127] Banning surreptitious peeping promises notice to the subject of when he is being watched; if the subject has no notice, then the peeping is banned. This approach envisions that the subject of surveillance may change boundary management mechanisms even within the sacred space of the home. For example, if a person has notice that his neighbors regularly and obviously look in his downstairs

---

124. *See* GA. CODE ANN. § 16-11-61(b) (West, Westlaw through 2015 Reg. Sess.) (defining "peeping Tom" as one "who peeps through windows or doors, or other like places . . . for the purpose of spying upon or invading the privacy of the persons spied upon and the doing of any other acts of a similar nature which invade the privacy of such persons"); LA. REV. STAT. ANN. § 14:284 (2014) (defining a Peeping Tom as "one who peeps through windows or doors, or other like places, situated on or about the premises of another for the purpose of spying upon or invading the privacy of persons spied upon without the consent of the persons spied upon"); VA. CODE ANN. § 18.2-130 (West, Westlaw through 2015 Reg. Sess.) (penalizing a person for peeping when he "secretly or furtively peep[s], sp[ies] or attempt[s] to peep or spy into or through a window, door or other aperture").

125. Lance E. Rothenberg, *Re-Thinking Privacy: Peeping Toms, Video Voyeurs, and Failure of the Criminal Law to Recognize a Reasonable Expectation of Privacy in the Public Space*, 49 AM. U. L. REV. 1127, 1140–43 (2011); Antonietta Vitale, Note, *Video Voyeurism and the Right to Privacy: The Time for Federal Legislation Is Now*, 27 SETON HALL LEGIS. J. 381, 389–90 (2002) ("Unfortunately, peeping statutes are few and far between and provide relief only for those few victims that actually catch Peeping Toms at their windows.").

126. *See* ARIZ. REV. STAT. ANN. § 13-1504 (2015) (defining "criminal trespass" as the illegal entering of a residential structure or yard, and the looking into a residence with "reckless disregard of infringing on the inhabitant's right of privacy"); DEL. CODE ANN. tit. 11, § 820 (West, Westlaw through 2015) (defining "trespassing with intent to peer or peep" as when a person "knowingly enters upon the occupied property or premises of another utilized as a dwelling, with intent to peer or peep into the window or door of such property or premises and who . . . otherwise acts in a manner commonly referred to as 'Peeping Tom'"; and defining a Peeping Tom as a trespasser who "knowingly enters upon the occupied property or premises of another . . . with intent to peer or peep into the window or door of such property or premises"); S.D. CODIFIED LAWS § 22-21-3 (2015) (defining "window peeking" as the entry onto private property to peep "in the door or window of any inhabited building or structure located thereon"); Rothenberg, *supra* note 125.

127. N.C. GEN. STAT. ANN. § 14-202 (West, Westlaw through 2015 Reg. Sess.) (defining "peeping" as looking secretly into a room occupied by another person); OKLA. STAT. ANN. tit. 21, § 1171 (West, Westlaw through 2015 1st Reg. Sess.) (defining a Peeping Tom as a "person who hides, waits or otherwise loiters in the vicinity of any . . . place of residence . . . with the unlawful and willful intent to watch, gaze, or look upon any person in a clandestine manner").

windows, he may choose to always come downstairs fully dressed. The notice-based law will not penalize his neighbors.

Voyeurism laws build on Peeping Tom laws. They penalize the viewing, photographing, or videotaping of another without consent.[128] Many state statutes limit the voyeurism offense to a particular sensitive subject matter: photographs of nudity, or of specific body parts.[129] Many states additionally limit the scope of the offense to surveillance conducted in physical locations where the subject can show a reasonable expectation of privacy.[130] Some states, as with intrusion or Peeping Tom laws, require trespass or surreptitious invasion.[131] A number of states require lascivious or sexual intent.[132]

These voyeurism offenses reinforce several kinds of boundary management. Like the intrusion tort and Peeping Tom statutes, they enforce boundary management that involves concealing oneself behind walls or in private locations or in privately-owned locations. In addition, they enforce notice and consent for such acts of observation or photography.

But in the late 1990s and early 2000s, it became apparent that privacy laws did not cover a new category of voyeurism offenses: the taking of "up-skirt" photographs or their equivalent in public spaces.[133] Many

---

128. Vitale, *supra* note 125, at 394–95.

129. *See, e.g.*, ALASKA STAT. ANN. § 11.61.123(a) (West, Westlaw through 2015 1st Reg. Sess.) ("A person commits the crime of indecent viewing or photography if, in the state, the person knowingly views, or produces a picture of, the private exposure of the genitals, anus, or female breast of another person and the view or production is without . . . knowledge or consent."); MO. ANN. STAT. § 565.253(1) (West, Westlaw through 2015 Veto Sess.) ("A person commits the crime of invasion of privacy if . . . [he] knowingly views, photographs or films another person, without that person's knowledge and consent, while the person being viewed, photographed or filmed is in a state of full or partial nudity and is in a place where one would have a reasonable expectation of privacy.").

130. *See, e.g.*, 18 PA. CONS. STAT. ANN. § 7507.1(a)(1) (West, Westlaw through 2015) (A person commits the offense of invasion of privacy if he knowingly "[v]iews, photographs, videotapes, electronically depicts, films, or otherwise records another person without that person's knowledge and consent while that person is in a state of full or partial nudity and is in a place where the person would have a reasonable expectation of privacy.").

131. OHIO REV. CODE ANN. § 2907.08(A)–(D) (West, Westlaw through 2015) (making it illegal to "commit trespass or otherwise surreptitiously invade the privacy of another" "for the purpose of sexually arousing or gratifying the person's self").

132. *See, e.g., id.*; WASH. REV. CODE § 9A.44.115(2) (2014) ("A person commits the crime of voyeurism if, for the purpose of arousing or gratifying the sexual desire of any person, he or she knowingly views, photographs, or films another person, without that person's knowledge and consent, while the person being viewed, photographed, or filmed is in a place where he or she would have a reasonable expectation of privacy.").

133. *See* Nancy Danforth Zeronda, Note, *Street Shootings: Covert Photography and Public Privacy*, 64 VAND. L. REV. 1131, 1134 (2010) (observing that "courts cling to conventional thinking

voyeurism statutes require the subject to be nude, and to be located in a private location.[134] The taking of photographs of a clothed subject in public spaces is not covered by these definitions.

So instead of focusing on the boundary management mechanism of walls, several states shifted to enforcing the boundary management mechanism of clothing. Illinois made it unlawful to videotape a person under or through clothing for the purpose of viewing the body or undergarments.[135] Ohio did the same a year later, penalizing surreptitious recording.[136] California also clarified that the offense covered recording under or through clothing, but limited it to "circumstances in which the other person has a reasonable expectation of privacy."[137]

Interestingly, these more recent voyeurism statutes show that courts and legislators can and will recognize some kinds of expectations of privacy even in a public space.[138] The federal Video Voyeurism Prevention Act of 2004 defines a reasonable expectation of privacy as a person's belief that a private area of the body will not be visible to the public, "regardless of whether that person is in a public or private place."[139]

Clothing usually functions as an effective boundary management

---

that invasions of privacy cannot occur in the public sphere. New and problematic forms of street photography necessitate a reexamination of photographic invasions of privacy").

134. *See, e.g.*, *id.* at 1144–45 (discussing *State v. Glas*, 147 Wash. 2d 410, 421–22, 54 P.3d 147, 154 (2002), a case in which the court read Washington's voyeurism statute not to include intrusions made in public); *see also* 18 PA. CONS. STAT. ANN. § 7507.1(a) (West, Westlaw through 2015) (penalizing recording "while that person is in a state of full or partial nudity and is in a place where that person would have a reasonable expectation of privacy").

135. 720 ILL. COMP. STAT. ANN. 5/26-4(a-10) (West, Westlaw through 2015 Reg. Sess.) ("It is unlawful for any person to knowingly make a video record or transmit live video of another person under or through the clothing worn by that other person for the purpose of viewing the body of or the undergarments worn by that other person without that person's consent.").

136. OHIO REV. CODE ANN. § 2907.08(D) (West, Westlaw through 2015) ("No person shall secretly or surreptitiously videotape, film, photograph, or otherwise record another person under or through the clothing being worn by that other person for the purpose of viewing the body of, or the undergarments worn by, that other person.").

137. CAL. PENAL CODE § 647(j)(2) (West, Westlaw through 2015 Reg. Sess.) ("Any person who uses a concealed camcorder . . . to secretly videotape, film, photograph, or record by electronic means, another, identifiable person under or through the clothing being worn by that other person, for the purpose of viewing the body of, or the undergarments worn by, that other person, without the consent or knowledge of that other person, with the intent to arouse, appeal to, or gratify the lust, passions, or sexual desires of that person and invade the privacy of that other person, under circumstances in which the other person has a reasonable expectation of privacy [will have violated this statute].").

138. *See* Kaminski, *supra* note 58, at 70.

139. Video Voyeurism Prevention Act of 2004, 18 U.S.C. § 1801(b)(5)(B) (2012).

mechanism when an individual is in public. The rise of low-cost, smaller, and less obtrusive recording devices that can be hidden in new vantage points means that in practice clothing has become a less effective boundary management tool. But to preserve the efficacy of clothing, and prevent individuals from having to resort to changed behavior, legislators stepped in. Voyeurism laws allow individuals to continue to rely on clothing as an effective means of preventing unwanted disclosure. These laws protect individuals (usually women) from dignitary harms, unwanted harassment, and impingement on self-expression; but they do so through enabling individuals to continue to rely on their clothes.

Interestingly, in Japan, technology companies volunteered a different solution to the voyeurism problem. In response to an uptick in up-skirt photography in Japan, cellular phone manufacturers agreed to make cellphone cameras play a shutter sound that could not be disabled by muting the phone.[140] In other words, they chose to provide notice, presumably to use social norms to restrict illicit photography and videography. This notice was not required by law, but was volunteered and coordinated between phone companies.[141] However, photographers bypassed this technological fix by downloading a "silent photo" smartphone application that removed the shutter sound, making it easier to take surreptitious pictures.[142] The limitations of technological solutions led to a discussion of legal solutions instead.[143]

Intrusion upon seclusion laws, Peeping Tom laws, and video voyeurism laws are inherently limited in scope. Because courts have largely limited the application of the intrusion tort to private spaces, state legislators have no guarantees that the tort will cover offenses that occur in public or those that are assisted by new technologies.[144] Peeping Tom

---

140. Akky Akimoto, *Google Glass May Shatter Japan's 'Manner' Mode*, JAPAN TIMES (May 15, 2013), http://www.japantimes.co.jp/life/2013/05/15/digital/google-glass-may-shatter-japans-manner-mode/#.VYDdSkbJJ—. ("[A]ll cellphones with built-in cameras shipped with a shutter sound that played when a photo was taken—and it could not be disabled. This was not something that was required by law, but it was taken up voluntarily by all Japanese cellphone vendors. These self-regulations have never been made publicly available, but NTT Docomo told The Japan Times that they implemented it to 'prevent secret filming or other privacy issues.'").

141. *Id.*

142. Masaki Karaya, *Rise in Sleazy Voyeurism Blamed on 'Silent Photo' Smartphone App*, THE ASAHI SHIMBUN (Feb. 7, 2013), http://ajw.asahi.com/article/behind_news/social_affairs/AJ201302070001.

143. *Id.*

144. *See* Dietemann v. Time, Inc., 449 F.2d 245 (9th Cir. 1971); Shulman v. Grp. W Prods., Inc., 955 P.2d 469 (Cal. 1998). But see, in the Fourth Amendment context, *Kyllo v. United States*, 533 U.S. 27 (2001), and *Florida v. Riley*, 488 U.S. 445 (1989). Intrusion upon seclusion might include

laws usually have physical limits built into the statute: that the offender has committed trespass or was caught at the window. Voyeurism laws are often limited to physical spaces, particularly sensitive subject matter, lascivious intent, or peering through clothing. Thus, this first category of boundary management laws can get overlooked as representing a more traditional conception of privacy.

The next two types of surveillance laws approach boundary management differently, reaching the ways in which newer technologies threaten an individual's ability to calculate her ideal degree of disclosure.

2. *Distance, Vantage Point, and "Sense Enhancement"*

A second type of law steps in when technology closes distances or makes it possible to observe someone from new vantage points. Distances can be closed through "sense enhancement": the use of a zoom lens, for example, or a microphone. Technology can also enable an observer to achieve new vantage points, such as observing an individual from overhead or underneath.

Both the closing of distances and the enabling of new vantage points disrupt traditional mechanisms of notice. These kinds of surveillance are less visible than physical trespass, or listening in on a conversation while remaining visible to the speaker. An individual may not be aware that he is being observed or recorded from a distance, through a wall, or from or a particular angle, and thus will miscalculate his ideal degree of disclosure.

This second type of law is not entirely distinct from the first type; many laws addressing sense-enhancing technologies are still concerned with the breach of a barrier surrounding a particular physical space. And some laws contain both concerns over the permeability of physical barriers and concerns over the closing of distance or adoption of unusual vantage points. But if the first type of law was concerned with the actual holes in a wall, this second type is concerned with technology that enhances human senses to create constructive holes in the wall.

Technologies like zoom lenses or thermal imaging allow watchers to transgress the same boundaries protected in Peeping Tom statutes

---

video voyeurism, for example, but has largely been ineffectively enforced. *See* RESTATEMENT (SECOND) OF TORTS § 652 cmt. c (1977) ("Even in a public place, however, there may be some matters about the plaintiff, such as his underwear or lack of it, that are not exhibited to the public gaze; and there may still be invasion of privacy when there is intrusion upon these matters."). *But see* Rothenberg, *supra* note 125 (noting that courts hesitate to find a reasonable expectation of privacy in public); Vitale, *supra* note 125.

without necessarily falling within the statutes' purview because a watcher does not need to trespass or to look through a window to gain access to the private space or private information.[145] California's paparazzi law provides a fascinating example of legal reinforcement of existing boundary management mechanisms that have become less effective in the face of new technologies. Until 2014, the California paparazzi law targeted the use of telephoto lenses or sense-enhancing audio technology to peer into or listen in on a privately-owned space.[146] The statute focused on preserving the integrity of a space that has traditionally been inaccessible, except by physical trespass, maintaining traditional boundary management mechanisms in a private space in the face of technological change. In 2014, the statute was amended to cover all technology used to peer into an area formerly inaccessible except by trespass, even if that technology is not sense-enhancing.[147] The amendment was purportedly passed to address the use of drones, which might take new perspectives (from the sky) without needing to employ sense-enhancing technologies.[148]

The intrusion tort has been used to address sense-enhancement technologies.[149] In a case addressing whether a videographer could be liable for recording a conversation between a car accident victim and a nurse, the California Supreme Court observed that "merely . . . being present at a place where he could hear such conversations with unaided ears" did not constitute a privacy violation.[150] But "placing a microphone on [the nurse's] person, amplifying and recording what she said and heard" could violate a reasonable expectation of privacy.[151] Using amplification to listen in on a conversation prevents the subject of surveillance from adjusting her degree of disclosure appropriately because it does not provide notice to the subject the way visibly standing

---

145. MODEL PENAL CODE § 221.2(3)(b) (1962) ("It is an affirmative defense . . . [that] the premises were at the time open to members of the public and the actor complied with all lawful conditions imposed upon access to or remaining in the premises.").

146. *See* CAL. CIV. CODE § 1708.8(b) (West 2011) (regulating recording where a "physical impression could not have been achieved without a trespass unless the visual or auditory enhancing device was used").

147. Assemb. 2306, 2013–2014 Reg. Sess. (Cal. 2014), *available at* http://leginfo.ca.gov/pub/13-14/bill/asm/ab_2301-2350/ab_2306_bill_20140930_chaptered.pdf; Cade, *supra* note 3.

148. *See* Melanie Mason, *California Assembly Approves Limits on Drones, Paparazzi*, L.A. TIMES (Jan. 29, 2014), http://www.latimes.com/local/political/la-me-pc-assembly-floor-bills-20140129-story.html.

149. *See* Shulman v. Grp. W Prods. Inc., 995 P.2d 469 (Cal. 1998).

150. *Id.* at 491.

151. *Id.*

nearby might.

Technology can also enable observation from unexpected vantage points. The voyeurism laws discussed earlier implicitly contemplate this problem.[152] While the laws do not explicitly target taking photographs or video from below a person, "up-skirt" photography is a problem precisely because it captures information from an unexpected vantage point.[153] It is far harder to manage one's expected degree of disclosure when the recording device is positioned to capture information from an unexpected angle.

Drones are discussed at greater length later in this Article, but the Texas drone statute provides an example of a law addressing both sense enhancement and vantage point and is thus worth mentioning here. Texas has made it illegal to use a drone "to capture an image of an individual or privately owned real property in this state with the intent to conduct surveillance on the individual."[154] An image does not fall into the statute's scope, however, if it was taken from a height of below eight feet above ground level in a public place, and without using technologies that enhance the senses "beyond normal human perception."[155] In other words, the statute encompasses only images taken from above eight feet high and using zoom or audio-enhancing technology. It targets observation from an unusually heightened vantage point, coupled with sense-enhancement. The further away the drone is, and the less observable it is, and the more able it is to observe a person without being seen. The more it is able to observe a person without being seen, the stronger the harm to that person's ability to accurately boundary manage. This suggests that if a person can see a drone, they can boundary manage accordingly and thus their privacy is not violated. But if the drone is further up, a person might not expect to be observed from that height, perspective, and zoom, and thus may fail to adequately boundary manage. By addressing the height of the drone, and its ability to amplify images, the Texas drone statute seeks to enable accurate boundary management by individuals. The Texas statute, however, is also riddled with exceptions for particular industries discussed at greater length below, making it a poor example of legislating, overall.[156]

---

152. *See supra* Part V.A.1.

153. *See* Zeronda, *supra* note 4, at 1132–33 ("As its name suggests, up-skirt photography involves taking pictures of women up their skirts.").

154. H.R. 912, 83d Leg., Reg. Sess. § 423.003 (Tex. 2013).

155. *Id.* § 423.002(15).

156. *Id.* § 423.002 (listing exceptions).

3. *Ephemerality*

A third type of surveillance law also addresses the impact of technology on the environment in which disclosures are made, but instead of addressing the increased permeability of walls, it focuses on technology's impact on expectations about human memory. Instead of addressing the visibility of the recording device, this type of law focuses on the way in which recording technology eliminates the ephemerality of the natural environment. A world without recording devices is more ephemeral in nature; people forget interactions, or fail to aggregate them and make connections or inferences.

Eavesdropping laws address recording technologies that change the environment in which boundary management decisions get made.[157] Some eavesdropping statutes, like the paparazzi statute, focus on the management of private physical spaces. But others preserve a different

---

157. Rothenberg, *supra* note 125, at 1142 n.67; *see, e.g.*, ALASKA STAT. ANN. § 13A-11-31(a) (West, Westlaw through 2015 1st Reg. Sess.) (describing "[c]riminal eavesdropping" as when a person intentionally uses a device to eavesdrop); CAL. PENAL CODE § 632(a) (West, Westlaw through 2015 Reg. Sess.) (defining "[e]avesdropping" as when a person "intentionally and without . . . consent . . . eavesdrops upon or records the confidential communication"); COLO. REV. STAT. § 18-9-304(1)(a)–(c) (West, Westlaw through 2015 1st Reg. Sess.) (defining "[e]avesdropping" as when a person not present for a conversation "[k]nowingly overhears or records such conversation or discussion without the consent . . . [or] for the purpose of committing, aiding, or abetting the commission of an unlawful act; or knowingly . . . attempts to use or disclose . . . the contents of any such conversation or discussion"); GA. CODE ANN. § 16-11-62(1) (West, Westlaw through 2015 Reg. Sess.) (defining "[e]avesdropping" as any attempt "in a clandestine manner intentionally to overhear, transmit, or record . . . the private conversation of another which shall originate in any private place"); KAN. STAT. ANN. § 21-4001 (West, Westlaw through 2015 Reg. Sess.) (defining "eavesdropping" as the intentional entry into a private place for the purpose of surreptitiously listening to private communications or observing private conduct); KY. REV. STAT. ANN. § 526.010 (West, Westlaw through 2015 Reg. Sess.) (describing "eavesdrop" as the intentional use of any device to "overhear, record, amplify or transmit any part of a wire or oral communication of others without the consent of at least one (1) party thereto"); MICH. COMP. LAWS ANN. § 28.807(2) (West, Westlaw through 2015 Reg. Sess.) (defining "eavesdropping" as the intentional trespass onto another's property or use of any device to "overhear, record, amplify or transmit any part of the private discourse of others without the permission of all persons engaged in the discourse"); N.Y. PENAL LAW § 250.05 (McKinney 2015) (describing "eavesdropping" as the unlawful "wiretapping, mechanical overhearing of a conversation, or interception or accessing an electronic communication"); N.D. CENT. CODE ANN. § 12.1-15-02 (West, Westlaw through 2015 Reg. Sess.) (defining "felony eavesdropping" as the intentional interception of any communication "by use of any electronic, mechanical, or other device," and "misdemeanor eavesdropping" as the secret lingering about a private place with "intent to overhear discourse or conversation therein"); OKLA. STAT. ANN. tit. 21, § 1202 (West, Westlaw through 2015 1st Reg. Sess.) (describing eavesdropping as "secretly loitering about any building, with intent to overhear discourse therein, and to repeat or publish the same to vex, annoy, or injure others"); S.D. CODIFIED LAWS § 22-21-1 (2015) (defining "eavesdropping" as a trespass with intent to eavesdrop in a private place, or an installation of any device for "observing, photographing, recording, amplifying or broadcasting sounds or events in such place").

kind of assumption about one's environment: the assumption that one's conversations, even outside of privately owned space, will not have staying power. Eavesdropping statutes address boundary management that is conducted based on experiences with ephemerality and human memory. If every conversation outside of the home may be recorded, then people may want to adjust the content, tone, and length of their conversations outside of the home to optimize social accessibility and disclosure.[158]

But eavesdropping statutes show that determining the level of appropriate state involvement in boundary management outside of the home is not simple. Many states require a reasonable expectation of privacy in the conversation.[159] This requirement ensures that conversations are protected only when the subject is in fact showing that she has a reasonable expectation of privacy by trying to employ other tools of boundary management. If you shout the conversation from a rooftop, chances are many will hear you and some may record you. In some states, if the recording device is in plain view, then the subject will be deemed to have consented to being recorded, even with no explicit consent.[160]

This makes sense in the framework of boundary management, because when the recording device is in plain view, the subject is given opportunity to adapt optimization behaviors accordingly. In public spaces, the state is not necessarily interested in preventing people from adapting their behavior to account for the presence of others. But it is interested in enabling people who believe they can rely on older forms of boundary management—talking in a lower voice, in a perceivably private space, without visible listeners—to have a fair chance to boundary manage appropriately, relying on those mechanisms.

Most states provide that conversations can be legally recorded with the consent of only one party.[161] This ensures that eavesdropping statutes do not impose additional boundary management mechanisms where there weren't mechanisms before. Before recording or eavesdropping technologies, a speaker in a conversation depended on the relationship with the other person to decide how much to reveal. False friends existed

158. *See* Bartnicki v. Vopper, 532 U.S. 514, 533 (2001); United States v. White, 401 U.S. 745, 787 (1971) (Harlan, J., dissenting); Am. Civil Liberties Union of Ill. v. Alvarez, 679 F.3d 583, 613–14 (7th Cir. 2012) (Posner, J., dissenting).

159. *See* Potere, *supra* note 4, at 283–84; Triano, *supra* note 4.

160. Potere, *supra* note 4, at 283.

161. *Id.* at 283 n.74.

long before cellphone recordings.[162] Thus many eavesdropping laws do not step in to ensure that friends will be more loyal. Those eavesdropping laws that require two-party consent and fail to require a reasonable expectation of privacy have been found most troubling by courts from a First Amendment perspective.[163]

Location-tracking also raises issues of ephemerality and permanence. Automated license plate readers (ALPRs) location-track individuals over time by photographing and analyzing license plates appearing on public roads. *The Wall Street Journal* revealed in 2014 that the government has been using ALPRs to track millions of individuals in real time.[164] Law enforcement's use of ALPRs raises questions similar to those raised by GPS, which the Supreme Court recently addressed in *United States v. Jones*.[165] But governing the private use of ALPRs moves into the relatively uncharted territory of balancing one entity's right to record against another's right to privacy.

Laws governing ALPR systems can be understood as governing boundary management. Location-tracking implicates boundary management over time and distance. Prior to technologies such as ALPRs and GPS, tracking a person over a long period of time was costly and involved both focus and effort.[166] A person could thus rely on practical obstacles to prevent location-tracking over time.[167] When legislators decide to step in to govern GPS use or ALPR use, they do so to impose legal friction where before practical friction prevented tracking.

At least two states have enacted laws governing the private use of ALPRs.[168] Utah initially enacted a law prohibiting a person from using an ALPR system.[169] The Utah statute defined an ALPR system as "a system of one or more mobile or fixed automated high-speed cameras used in combination with computer algorithms to convert an image of a

---

162. *See, e.g.*, United States v. White, 401 U.S. 745 (1971); Lopez v. United States, 373 U.S. 427 (1963).

163. *See, e.g.*, *Alvarez*, 679 F.3d 583 (analyzing Illinois's two-party-consent wiretap law under the First Amendment).

164. Devlin Barrett, *U.S. Spies on Millions of Drivers*, WALL ST. J. (Jan. 26, 2015), http://www.wsj.com/articles/u-s-spies-on-millions-of-cars-1422314779.

165. United States v. Jones, __ U.S. __, 132 S. Ct. 945 (2012).

166. *See, e.g.*, *id.* at 955–56 (Sotomayor, J., concurring), 963–64 (Alito, J., concurring).

167. *See generally* Kevin S. Bankston & Ashkan Soltani, *Tiny Constables and the Cost of Surveillance: Making Cents out of* United States v. Jones, 123 YALE L.J. ONLINE 335 (2014).

168. S. 0196, 2013 Gen. Sess., Reg. Sess. (Utah 2013); S. 2141, 188th Gen. Court, Reg. Sess. (Mass. 2014).

169. Utah S. 0196.

license plate into computer-readable data."[170]

However, shortly after enactment of this law, Utah was sued by ALPR companies for violating their First Amendment rights.[171] In reaction, Utah heavily amended the law to allow private entities to collect license plate information, sell it to third parties, and hold it for up to nine months.[172]

Arkansas also enacted a license plate reader law.[173] Perhaps unsurprisingly, given the effectiveness of such an action in Utah, Arkansas has also been sued for First Amendment violations.[174] The Massachusetts legislature has proposed an ALPR law, but as of January 2015, the law has been sitting with the Senate.[175]

B. Determining the Strength of the Legislative Interest

Framing surveillance laws as protecting boundary management allows for at least two types of government interests, as discussed: an interest in notifying people in order to enable boundary management, and an interest in preventing a shift to other kinds of less desirable behaviors. The government interest in notifying people that they are being recorded is strong, and nicely tailored to enabling boundary management. It may raise interesting questions related to anonymous speech—does one have a right to record surreptitiously, where announcing that one is recording would prevent the recording from occurring?[176] But the idea that states may require notice of recording should be understandable to courts as an interest in enabling boundary management in a shifting environment.

Other surveillance laws instead aim to preserve a genre of boundary management and prevent a shift in behavior. Understanding statutes this way can allow courts to focus on the strength of the government interest in preventing a particular shift, or set of shifts, in behavior, instead of

---

170. *Id.*

171. Complaint, Digital Recognition Network, Inc. v. Herbert, No. 2:14-cv-00099 (D. Utah Feb. 13, 2014).

172. S. 222, 2014 Gen. Sess., Reg. Sess. (Utah 2014), *available at* http://le.utah.gov/~2014/bills/static/SB0222.html.

173. ARK. CODE ANN. §§ 12-12-1801–1808 (West, Westlaw through 2015 Reg. Sess.).

174. Complaint, Digital Recognition Network, Inc. v. Beebe, No. 4:14-cv-00327 (E.D. Ark. May 30, 2014); *License Plate Reader Makers Sue Arkansas for Banning Their Tech*, RT QUESTION MORE (June 18, 2014, 11:27 PM), http://rt.com/usa/166916-vigilant-drn-arkansas-alpr-lawsuit/.

175. *See* S. 2141, 188th Gen. Court, Reg. Sess. (Mass. 2014).

176. *See* McIntyre v. Ohio Elections Comm'n, 514 U.S. 334 (1995) (finding First Amendment protection for distribution of anonymous petitions).

identifying an amorphous notion of privacy. This may raise interesting tailoring issues, questioning how narrowly states will have to tailor statutes to prevent particular shifts, versus preserving a traditionally protectable genre of behavior, such as boundary management in the home.

C. *Identifying the First Amendment Interest in Privacy Protection*

Privacy laws can run into First Amendment problems, but they can also be essential to First Amendment interests.[177] The boundary management framework demonstrates how this works in practice. As previously described, boundary management studies suggest that people increase disclosure when they trust that information will not move beyond an expected boundary from trusted parties to untrustworthy people.[178] When a trusted boundary instead becomes permeable, people may decrease disclosure. This decrease in disclosure can often be articulated as a decrease in speech. In other words, if law does not step in to reinforce the formerly trusted boundary, people will speak less, or less frankly, resorting to lying or omission as boundary management tactics.

Courts are already receptive to this idea of the relationship between privacy and free speech. In *Bartnicki v. Vopper*,[179] a case about whether a radio station could distribute an illegally wiretapped conversation, the Supreme Court recognized that there were speech interests on both sides of the case.[180] The majority recognized that if people are unable to trust that an intimate conversation is in fact intimate, they may speak less.[181]

In the earlier Fourth Amendment case of *United States v. White*,[182] both Justice Harlan and Justice Douglas noted in dissents that allowing electronic eavesdropping by an undercover agent could have significant First Amendment implications. Justice Harlan explained that off-hand conversations are usually made to a limited audience, and are easily forgotten. People rely on these features of their environment to manage how open they are in conversation.[183] In the absence of legal protection

---

177. *See generally* Neil M. Richards, *Intellectual Privacy*, 87 TEX. L. REV. 387 (2008); Kaminski & Witnov, *supra* note 59.

178. DERLEGA & CHAIKIN, *supra* note 97, at 104.

179. 532 U.S. 514 (2001).

180. *Id.* at 533.

181. *Id.* ("[T]he fear of public disclosure of private conversations might well have a chilling effect on private speech.").

182. 401 U.S. 745 (1971).

183. *Id.* at 788 (Harlan, J., dissenting) ("Much off-hand exchange is easily forgotten and one may

from permanent recordings, people will regulate the content of their conversations and disclose less.[184] Justice Douglas more directly identified this as a First Amendment problem. He focused on loss of spontaneity: "Monitoring, if prevalent, certainly kills free discourse and spontaneous utterances."[185]

Judge Posner, dissenting in a recent Seventh Circuit case on the First Amendment right to record, similarly noted that eavesdropping laws protect First Amendment values.[186] Judge Posner noted that people would be less likely to disclose useful information to the police if there is no law protecting public conversations with police officers from being recorded.[187] Judge Posner has been a vocal critic of privacy.[188] But he seemed very receptive to the idea that electronic eavesdropping laws prevent people from resorting to socially undesirable boundary management techniques. Posner explained that electronic recording can eliminate communicative spontaneity, quoting Justice Harlan's dissent in *White*: "[W]ords would be measured a good deal more carefully and communication inhibited if one suspected his conversations were being transmitted and transcribed."[189] And interestingly, Posner understood the eavesdropping law as stepping in to preserve a genre of communication—off-hand communication in public in the absence of recording devices. He cited Justice Harlan for the proposition that poor human memory, a limited audience, and the relative anonymity most people enjoy in public spaces usually preserve the obscurity of off-hand conversations.[190] Electronic recording disrupts that natural obscurity and

---

count on the obscurity of his remarks, protected by the very fact of a limited audience, and the likelihood that the listener will either overlook or forget what is said, as well as the listener's inability to reformulate a conversation without having to contend with a documented record.").

184. *Id.* at 787 ("[W]ords would be measured a good deal more carefully and communication inhibited if one suspected his conversations were being transmitted and transcribed.").

185. *Id.* at 762.

186. Am. Civil Liberties Union of Ill. v. Alvarez, 679 F.3d 583, 611 (7th Cir. 2012) (Posner, J., dissenting)

187. *Id.* (noting that finding the Illinois eavesdropping statute to violate the First Amendment "is likely to impair the ability of police both to extract information relevant to police duties and to communicate effectively with persons whom they speak with in the line of duty").

188. Ronald K.L. Collins, *On Privacy, Free Speech, & Related Matters—Richard Posner vs David Cole & Others*, CONCURRING OPINIONS (Dec. 15, 2015), http://concurringopinions.com/archives/2014/12/on-privacy-free-speech-related-matters-richard-posner-vs-david-cole-others.html.

189. *Alvarez*, 679 F.3d at 612.

190. *Id.* (quoting Justice Harlan's dissent in *White*, 401 U.S. at 787–88); *see also id.* at 613–14 ("[P]rivate talk in public places is common, indeed ubiquitous, because most people spend a lot of their time in public places; because they rely on their anonymity and on the limited memory of others to minimize the risk of publication; because public places are (paradoxically) often more private than private places (imagine if detectives could meet with their informants only in police

causes people to speak and behave in more conservative ways.[191] Posner thus identified that the state's eavesdropping statute in fact promotes a First Amendment interest in conversational privacy, even in public spaces.[192] While the majority did recognize a First Amendment interest in conversational privacy, it explained that the statute was drafted too broadly to survive First Amendment scrutiny.[193]

Courts evaluating privacy torts have similarly noted that failure to legally reinforce the expected boundaries of conversations could lead to more inhibited conversations, with negative social consequences. In *Dietemann v. Time*,[194]—a Ninth Circuit case about whether the First Amendment protected reporters who recorded their interactions with a quack doctor—the court found that surreptitious electronic recording violated the plaintiff's privacy despite the fact that reporters had permission to be on the premises.[195] The court explained that a "different rule . . . would surely lead to guarded conversations and conduct where candor is most valued, *e.g.*, in the case of doctors and lawyers."[196] A doctor who could be surreptitiously recorded might not be honest with her patient; she might boundary manage through discretion or even dishonesty, out of fear that the expected boundary external to her patient relationship might be breached through recording. The court's reasoning in this is somewhat backwards, since usually it's the patient's privacy and need for candor that provokes concern. Nonetheless, the Ninth Circuit appeared to recognize that legal protection of boundary management can encourage freer speech within a protected

---

stations); and because eavesdropping on strangers is actually rather uncommon because it is so difficult in most cases to understand a conversation between strangers.").

191. *Id.* at 613 (citing Lizette Alvarez, *Spring Break Gets Tamer as World Watches Online*, N.Y. TIMES, March 16, 2012, at A10).

192. *Id.* ("There is more on the state's side of this case than privacy of communications and the effectiveness of law enforcement—and the more is the same First Amendment interest that the ACLU says it wants to promote. The majority opinion concedes that 'conversational privacy' 'serves First Amendment interests,' but thinks there can be no conversational privacy when the conversation takes place in a public place . . . ."); *see also id.* at 614 ("[O]n the other side of the balance are the inhibiting effect of nonconsensual recording of conversations on the number and candor of conversations (and hence on values that the First Amendment protects) . . . .").

193. *Id.* at 608 ("[W]e have acknowledged the importance of conversational privacy and heeded the basic distinction drawn in *Katz* that some conversations in public places implicate privacy and others do not . . . . But the Illinois eavesdropping statute obliterates the distinction between private and nonprivate by criminalizing *all* nonconsensual audio recording *regardless* of whether the communication is private *in any sense*." (emphasis in original)).

194. 449 F.2d 245 (9th Cir. 1971).

195. *Id.* at 249.

196. *Id.*

conversation. This internalization of First Amendment rights within a privacy law could help such laws better withstand First Amendment scrutiny.

D. Guiding the Enactment of New Laws

Understanding the state's interest in surveillance laws as an interest in boundary management should enable legislators to enact new, legitimate, and appropriately tailored laws. If a legislature decides that its interest is in enabling people to effectively boundary manage in a particular context, then it can devise a statute that focuses on requiring notice to the individual. If instead a legislature worries about the pernicious effects of behavioral shifts—such as wearing protective clothing (up-skirt laws) or having less truthful and open conversations (eavesdropping laws)—then it can enact laws that reinforce particular genres of boundary management.

The particular state interest is important because emerging technologies will inspire more boundary management laws. Some of the issues will be familiar: for example, the governance of location tracking over time, or the governance of intrusion into intimate spaces. Other issues will be newer: for example, the use of robotic faces to manipulate trust.

This section reviews the recent enactment of drone privacy laws as an example of how drafting laws around the boundary management interest can make for better laws. Then it discusses the appropriateness of the boundary management framework for devising new privacy laws to govern robotics.

1. Drone Laws as an Example

Recent technological developments have inspired states to enact new laws governing information gathering by drones, or unmanned aerial vehicles (UAVs). Ryan Calo famously referred to drones as "privacy catalysts," predicting that drones would force a public conversation about many of the privacy violations scholars have been discussing for decades.[197] And, in fact, multiple states have enacted drone privacy laws, both to govern law enforcement use of drones (which is outside of the scope of this Article), and to govern private drone use.[198]

---

197. Calo, *supra* note 22, at 32.

198. *See, e.g.*, FLA. STAT. ANN. § 934.50 (West, Westlaw through 2015 1st Reg. & Sp. A Sess.); IDAHO CODE ANN. § 21-213 (West, Westlaw through 2015 Reg. Sess.); 725 ILL. COMP. STAT. ANN. 167 / 1-40 (West, Westlaw through 2015 Reg. Sess.).

This state-by-state approach allows experimentation with privacy legislation, and will allow courts to determine how best to balance statutes protecting privacy against the burgeoning First Amendment right to record.[199] Interestingly, many of these state laws governing private drone use have been enacted before the FAA officially permitted commercial use of drones.[200] States have been anticipating drone-related privacy problems rather than waiting for the technology to be widely commercially used.

State drone statutes vary considerably. Some clearly articulate a boundary management interest, while others more clearly reflect haphazard lobbying. The closer a state hews to enabling boundary management, the better the Legislature is able to justify the law's existence, and the more legitimate the law appears. Drone privacy laws thus illustrate how boundary management principles might guide the enactment of new privacy laws, and help legislators avoid the pitfalls of more haphazard legislation.

The Texas Legislature passed one of the more clearly haphazard drone statutes. At its core, however, the statute can be understood as addressing boundary management. Texas was one of the first states to enact a statute governing private drone use.[201] Texas puts a protective privacy halo around both private property and persons.[202] It prohibits the use of drones to capture images of individuals or real property with the "intent to conduct surveillance."[203]

The Texas Legislature did not stick to protecting boundary management. A remarkable number of the many exceptions to the law are clearly legislative carve-outs for specific industries, including oil and real estate, and interestingly do not include newsgathering or journalism.[204] The haphazard nature of these exceptions could be

199. Kaminski, *supra* note 58 (encouraging experimentation).

200. The FAA has authorized some commercial companies to use drones through the Section 333 process, but otherwise commercial drone use as of this draft is federally banned. Hobbyists may use drones within line of sight and under 400 feet. *See Civil Operations (Non-Governmental)*, FED. AVIATION ADMIN., https://www.faa.gov/uas/civil_operations/ (last modified Mar. 17, 2015, 10:42 AM); *Model Aircraft Operations*, FED. AVIATION ADMIN., https://www.faa.gov/uas/model_aircraft/ (last modified Mar. 4, 2015, 1:17 PM).

201. *See* H.R. 912, 83d Leg., Reg. Sess. (Tex. 2013).

202. TEX. GOV'T CODE ANN. § 423.003 (West, Westlaw through 2015 Reg. Sess.).

203. *Id.* The statute says "intent" has the meaning assigned to it by Section 6.03 of the Penal Code. That section defines intent versus negligence versus knowingly, but doesn't define "surveillance." *See* TEX. PENAL CODE ANN. § 6.03 (West, Westlaw through 2015 Reg. Sess.).

204. For example, there are carve-outs for real estate and oil pipeline inspections. TEX. GOV'T CODE ANN. § 423.002(13), (18).

deemed content-based or viewpoint-based regulation under First Amendment analysis,[205] and problematically reflects unequal treatment due to lobbying.

The Idaho drone law is broad, and aimed at privacy violations rather than solely at trespass.[206] It prohibits the intentional surveillance by drone of "specifically targeted persons or specifically targeted private property."[207] The term "surveillance" is not defined in the statute, but may be read by courts to indicate a temporal requirement, which would implicate boundary management over time.

The Idaho law again nods at the coextensiveness of physical and social boundaries, banning surveillance of an individual or a dwelling and its curtilage. A second cause of action bans the use of a drone "to photograph or otherwise record an individual . . . for the purpose of publishing or otherwise publicly disseminating such photograph or recording."[208] Rather than addressing boundary management over time, this addresses boundary management in the number of people one intends information to flow to. Interestingly, the Idaho drone law exempts drones used for mapping and resource management,[209] suggesting that incidental recording may not breach privacy interests.

However, the Idaho law, like the Texas law, reflects obvious lobbying. The Legislature singled out farms, ranches, and dairies for protection.[210] The singling out of particular groups for protection, just like the singling out of particular groups as exempt from the Texas statute's coverage, could pose content-based regulation problems under the First Amendment.

Tennessee enacted two drone laws in 2014. The first is a hunting law, making it a misdemeanor for a person to use a drone "to conduct video surveillance of private citizens who are lawfully hunting or fishing."[211] Illinois has enacted a similar law, protecting hunters.[212]

The second Tennessee drone law mirrors Texas's law.[213] The

---

205. *See* Sorrell v. IMS Health Inc., __ U.S. __, 131 S. Ct. 2653, 2663 (2011).

206. *See* IDAHO CODE ANN. § 21-213 (West, Westlaw through 2015 1st Reg. & 1st Extraordinary Sess.).

207. *Id.* § 21-213(2)(a).

208. *Id.* § 21-213(2)(b).

209. *Id.* § 21-213(1)(b)(ii).

210. *Id.* § 21-213(2)(a)(ii). The Idaho statute also exempts model planes "used purely for sport or recreational purposes." *Id.* § 21-213(1)(b)(i).

211. TENN. CODE ANN. § 70-4-302 (West, Westlaw through 2015 1st Reg. Sess.).

212. *See* 720 ILL. COMP. STAT. § 5 / 48-3(b)(10) (West, Westlaw through 2015 Reg. Sess.).

213. S. 1892, 108th Gen. Assemb., Reg. Sess. (Tenn. 2014) (codified at TENN. CODE ANN. § 29, 39-13).

Tennessee drone law makes it a class C misdemeanor to use a drone to "capture an image" of an individual or real property with the intent to conduct surveillance.[214] The law also bans knowing use of the image; possessing the image; and disclosing, displaying, distributing, or otherwise using the image after capturing it.[215] The law could be understood as concerned with contextual integrity, as destruction of the image before distribution is a defense.[216] Like the Texas law, the Tennessee drone statute is riddled with exceptions, excepting oil pipeline use, well safety, and research use.[217] The Oregon drone law takes a different approach; it hews closely to real property rights.[218] Rather than addressing surveillance per se, it addresses "trespass by a drone."[219] The Oregon drone law creates a private right of action for anybody who "owns or lawfully occupies real property" against a person conducting drone flight over that property.[220] Initially, drone trespass was limited to 400 feet above the property, but Oregon has since amended the statute to cover any overhead flight.[221] If one understands this trespass action as enforcing a privacy right, then this approach is similar to the California anti-paparazzi law, in that it considers low-flying drones to unacceptably disrupt boundary management taking place within and around the home. The Oregon law thus preserves whatever genre of boundary management a person uses on her own property, or property she lawfully occupies. Oregon legislators may have adopted the property-based approach to avoid potential First Amendment problems raised by the right to record, or may truly have considered the trespass-like aspect of drone flight more problematic. However, the law fails to address privacy violations that occur from drones operated away from an individual's property, with sense-enhancing technologies.

The Oregon statute includes additional requirements. The drone must have been flown over the property on at least one additional occasion, and the property owner or occupier must have notified the drone operator that she did not wish the drone to be flown again in that

214. *Id.* § 4(a).

215. *Id.* § 5(a)(2)(B) (Class B misdemeanor).

216. *Id.* § 4(c).

217. *Id.* § 3.

218. H.R. 2710, § 15, 77th Leg., Reg. Sess. (Or. 2013) (codified as amended by H.R. 2354, 78th Leg., Reg. Sess. (Or. 2015), at OR. REV. STAT. § 837.380 (2014)).

219. *Id.* at § 15(3).

220. OR. REV. STAT. ANN. § 837.380(1) (West, Westlaw through 2015 Reg. Sess.).

221. H.R. 2354, § 11, 78th Leg., Reg. Sess. (Or. 2015) (codified at OR. REV. STAT. § 837.380).

manner.[222] Oregon thus requires the potential plaintiff to actively engage in social boundary management, by contacting the drone operator, before a legal action can be brought. The law is brought in to enforce boundary management only after notice is provided to the drone operator.

The Wisconsin drone statute makes it a misdemeanor to use a drone to "photograph, record, or otherwise observe another individual in a place or location where the individual has a reasonable expectation of privacy."[223] The statute does not define whether that place is in private or in public. Like the tort of intrusion, this leaves many decisions in the hands of courts. But by targeting drones as the recording tool, the Wisconsin legislature might be nudging courts towards addressing the boundary management problems raised by drones: surreptitious recording, by a non-party to an interaction, from vantage points not formerly achievable by most people, or at least not without great cost.

2. *Robots and the Not-So-Distant Future*

If drones are the privacy problem of today, robots are the problem of the not-so-distant tomorrow. Robots in the home raise a slew of fascinating boundary management problems.[224] Robots are technologies that sense, process, and act in physical space.[225] People often rely on walls and social boundaries to ensure that the home is particularly private. If people permit robots into the home, even for limited tasks, then external walls no longer protect them from the broadcasting of a large amount of intimate information to third parties. Legislatures and courts will have to decide the extent to which permitting household robots into intimate spaces where relatively uninhibited behavior occurs extinguishes a privacy interest. This is no longer a question of whether information gathered in public can be considered private, but whether information gathered in private spaces by entities that have permission to be there can be considered private.[226] In other words, it is a question of

---

222. *Id.* at § 15(1)(a)–(b).

223. WIS. STAT. ANN. § 942.10 (West, Westlaw through 2015).

224. Ryan Calo, *Robots and Privacy*, *in* ROBOT ETHICS: THE ETHICAL AND SOCIAL IMPLICATIONS OF ROBOTICS (Patrick Lin et al. eds., 2010) (not identifying problem as boundary management, but identifying a number of the privacy issues raised by robots: direct surveillance, increased access, and social meaning); *see also* Margot E. Kaminski, *Robots in the Home: What Will We Have Agreed To?*, 51 IDAHO L. REV. 661 (forthcoming 2015).

225. *See* Calo, *supra* note 24.

226. For a longer discussion of these issues of consent versus genre protection, see Kaminski, *supra* note 224.

whether courts and legislators will decide to protect the genre of boundary management that takes place in the home—or bear the social costs that come from shifts in behavior in traditional locations of privacy protection.

Moreover, robots are not static: They will be able to move within homes, and transgress boundaries that prevent a static camera from peering around a corner. Governments will need to assess whether mobility poses a different threat to boundary management than static but continuous recording.

Additionally, as both Kate Darling and Ryan Calo have pointed out, to great effect, robots have a social dimension.[227] Humans innately react to faces, and a considerable amount of research is going in to how robotic faces, voices, and movements drive human reactions.[228] A well-known older study showed that humans read intent and emotion into mere motion patterns.[229] And humans can feel objects to be worthy of compassion, based on the object's design. When a robotics company released a video of its robot dog being kicked repeatedly, viewers voiced moral concerns with the perceived abuse.[230] The *New York Times* ran a heartbreaking video about the demise of Aibo robot dogs, showing owners holding funerals and mourning their lost pets.[231] Soldiers have expressed feelings of anger and loss at the "death" of bomb-defusing robots.[232] The ability to manipulate human reactions can also have troubling reverberations with the enforcement of long-held stereotypes. A study showed that people trust artificial speakers with deeper, more male-like voices as more authoritative, but would rather reveal intimate

---

227. Calo, *supra* note 24, at 119 (on file with author). *See generally* Darling, *supra* note 24 (arguing that because people tend to anthropomorphize robots, we should consider granting some kinds of legal protections to robots).

228. *See* Calo, *supra* note 24.

229. *See* Yann Leroux, *An Experimental Study of Apparent Behavior. Fritz Heider & Marianne Simmel. 1944*, YOUTUBE (Dec. 26, 2010), https://www.youtube.com/watch?v=n9TWwG4SFWQ.

230. Victoria Woollaston, *Is It Cruel to Kick a Robotic Dog? Google Video Reignites Debate over Whether Machines Should Be Treated Like Living Animals*, DAILY MAIL ONLINE (Feb. 16, 2015, 7:56 AM), http://www.dailymail.co.uk/sciencetech/article-2955544/Would-kick-robotic-dog-Google-video-regnites-debate-machines-treated-like-living-animals.html.

231. Jonathan Soble, *A Robotic Dog's Mortality*, N.Y. TIMES (June 17, 2015), http://www.nytimes.com/2015/06/18/technology/robotica-sony-aibo-robotic-dog-mortality.html.

232. Doree Armstrong, *Emotional Attachment to Robots Could Affect Outcome on Battlefield*, UW TODAY (Sept. 17, 2013), http://www.washington.edu/news/2013/09/17/emotional-attachment-to-robots-could-affect-outcome-on-battlefield/; Meghan Neal, *Are Soldiers Getting Too Emotionally Attached to War Robots?*, MOTHERBOARD (Sept. 18, 2013, 2:30 PM), http://motherboard.vice.com/blog/are-soldiers-getting-too-emotionally-attached-to-war-robots.

information to a higher, more female-like voice.[233]

These stories and studies suggest that human-robot interaction will operate at a higher level of social attachment and engagement than our interactions with, say, closed-circuit television (CCTV) cameras. Companies can and will use robot faces, voices, and movements to gain human trust. One form of boundary management is to evaluate how much one can rely on the person to whom one is talking. If robots can manipulate our assessment of the strength of our relationships with them, then legislators or courts may wish to step in to strengthen those boundaries through law.[234]

The Internet of Things, or adding sensors and connectivity to regular household objects, raises a perhaps more immediate version of a similar problem. If people are surrounded at home by objects that read to them as physical objects rather than cameras—such as the smart refrigerator—then they may continue to boundary manage as though their home objects were not recording. While robots may manipulate human emotions to gain trust, smart objects may manipulate human reactions by remaining calculatedly invisible. Legislators may wish to step in to either require some form of repeated notice, to enable appropriate boundary management in formerly private spaces, or may again wish to preserve certain genres of boundary management to prevent undesirable behavioral shifts by banning recording.

Smart objects also raise the interesting question of whether other-sense-employing recorders raise a new kind of notice issue. People adapt their behavior when they believe they are being watched—and a pair of eyes can cue that watching is occurring.[235] But are people able to adapt their behavior appropriately if the observation takes place on a different sensory dimension—such as, for example, heat-sensing? We may end up finding that notice works to enable effective boundary management with respect to certain kinds of information-gathering, but not with respect to other, non-visual or non-auditory forms. We may find that we are not able to boundary manage well when the breach takes place using other senses.

---

233. AARON POWERS ET AL., ELICITING INFORMATION FROM PEOPLE WITH A GENDERED HUMANOID ROBOT (2013), *available at* http://www.cs.cmu.edu/~kiesler/publications/2005pdfs/eliciting-information-people-gendered-humanoid-robot.pdf.

234. Woodrow Hartzog has suggested that the FTC is positioned to regulate such "unfair" behavior by robots under its Section 5 authority. *See* Woodrow Hartzog, *Unfair and Deceptive Robots*, 74 MD. L. REV. 785, 793–94 (2015).

235. Melissa Bateson et al., *Cues of Being Watched Enhance Cooperation in a Real-World Setting*, *in* 2 BIOLOGY LETTERS 412, 412 (2006).

This Article proposes that we should understand the government interest in preventing others from looking through walls and from having a perfect memory as the same underlying interest in enabling or preserving boundary management. Courts can be sympathetic to this interest. As new technologies raise new boundary management challenges, legislators should be more aware of the interests they wish to protect.

CONCLUSION

Understanding privacy as boundary management certainly is not limited to the private surveillance context. The boundary management conception of privacy could, and at least occasionally does, work in the Fourth Amendment context as well.[236]

But when it comes to laws governing surveillance by private actors, a boundary management framework fits particularly well. It helps explain both what is happening in these laws, and how they might be improved to better serve a legitimate legislative interest. Boundary management as a framework benefits from being descriptively accurate, and provides theoretical guidance to prevent piecemeal laws and guide the scope of new laws. In addition, the framework sets up privacy laws to be weighed, as they inevitably will be, against other values such as freedom of speech.

Reconciling the burgeoning right to record with the government's ability to govern intrusive information gathering is necessary as we move from a world of photographs and cellphone recordings to one where individuals are increasingly watched and quantified by drones, the Internet of Things, and even household robots. Real-world information capture will only become more prevalent; the physical spaces where we retreat from the online world will become less and less private, and the physical tactics we use to shield ourselves will become less and less effective. The problems of information privacy are increasingly appearing in the physical world, returning us to Warren and Brandeis's original fear that we will be recorded when we wish to be let alone.

---

236. *See, e.g.*, United States v. Jones, __ U.S. __, 132 S. Ct. 945, 956 (2012) (Sotomayor, J., concurring) ("GPS monitoring—by making available at a relatively low cost such a substantial quantum of intimate information about any person whom the Government, in its unfettered discretion, chooses to track—may 'alter the relationship between citizen and government in a way that is inimical to democratic society.'" (citation omitted)).