Privacy, Visibility, Transparency, and Exposure

Julie E. Cohen†

INTRODUCTION

This essay considers the relationship between privacy and visibility in the networked information age. Visibility is an important determinant of harm to privacy, but a persistent tendency to conceptualize privacy harms and expectations in terms of visibility has created two problems. First, focusing on visibility diminishes the salience and obscures the operation of nonvisual mechanisms designed to render individual identity, behavior, and preferences transparent to third parties. The metaphoric mapping to visibility suggests that surveillance is simply passive observation rather than the active production of categories, narratives, and norms. Part I explores this problem and identifies some of the reasons that US privacy jurisprudence has been particularly susceptible to it.

Second, even a broader conception of privacy harms as a function of informational transparency is incomplete. Privacy has a spatial dimension as well as an informational dimension. The spatial dimension of the privacy interest, which I characterize as an interest in avoiding or selectively limiting exposure, concerns the structure of experienced space. It is not negated by the fact that people in public spaces expect to be visible to others present in those spaces, and it encompasses both the arrangement of physical spaces and the design of networked communications technologies. US privacy law and theory currently do not recognize this interest at all. Part II argues that they should. Part III argues that the spatial dimension of the privacy interest extends to online conduct and considers some implications of that view for current debates about expectations of privacy online. Part IV offers some preliminary thoughts on how the privacy interest against exposure might affect thinking about privacy self-defense.

† Professor of Law, Georgetown University Law Center. Thanks to Susan Cohen, Oscar Gandy, Ian Kerr, David Phillips, Neil Richards, Rebecca Tushnet, participants in the Unblinking Workshop at UC Berkeley, and participants in The University of Chicago Law School's Surveillance Symposium for their comments on an earlier version of this paper, to Kirstie Ball for sharing her work in progress on exposure as an organizing concept for surveillance, and to Amanda Kane and Christopher Klimmek for research assistance.

I. VISIBILITY AND TRANSPARENCY

Within US legal culture, debates about privacy traditionally have reflected a relatively great concern with visibility and visual privacy issues. Over the last decade, the principal contribution of what has been dubbed the "information privacy law project"[1] has been to refocus both scholarly and popular attention on the other ways in which contemporary practices of surveillance operate to render individuals and their behaviors accessible in the networked information age. Yet the information privacy law project remains more closely tied to visibility than this description would suggest; its principal concern has been with data trails made visible to others. And to the extent that the information privacy law project conceptualizes privacy interests as interests against informational accessibility, its grasp of the workings and effects of surveillance is incomplete. Surveillance is only partly about the gathering and dissemination of fixed, preexisting information about identified individuals. Designations like "at risk," "no-fly," "soccer moms," "business elite," and "shotguns and pickups" are not preexisting facts. Surveillance also depends importantly on other, information-creating activities that lie outside the frame of visibility altogether.

An implicit linkage between privacy and visibility is deeply embedded in privacy doctrine. Within the common law of privacy, harms to visual privacy and harms to information privacy are subject to different requirements of proof. Of the four privacy torts, two are primarily visual and two primarily informational. The visual torts, intrusion upon seclusion and unauthorized appropriation of name or likeness, require only a showing that the conduct (the intrusion or appropriation) violated generally accepted standards for appropriate behavior.[2] The informational torts, unauthorized publication and false light, are far more stringently limited (to "embarrassing" private facts and to falsity).[3] To make out a more general claim to information privacy, some have tried to characterize collections of personally identified data visually, likening them to "portraits" or "images," but courts have resisted the conflation of facts with faces.[4] The body of constitutional privacy doctrine that defines unlawful "searches" regulates tools that enable law enforcement to "see" activities as they are taking place

1 Neil M. Richards, *The Information Privacy Law Project*, 94 Georgetown L J 1087 (2006). I should note that I am one of the scholars identified with this project.

2 See W. Page Keeton, et al, *Prosser and Keeton on the Law of Torts* § 117 at 851–56 (West 5th ed 1984).

3 See id § 117 at 856–66.

4 See, for example, *US News & World Report, Inc v Avrahami*, 1996 WL 1065557, *6–7 (Va Cir Ct); *Dwyer v American Express Co*, 652 NE2d 1351, 1355–56 (Ill App Ct 1995); *Castro v NYT Television*, 851 A2d 88, 98 (NJ Super Ct 2004).

inside the home more strictly than tools for discovering information about those activities after they have occurred.[5]

Within the academic literature on privacy, efforts to develop an account of privacy interests in personal information have confronted great skepticism, for reasons that seem closely linked to conventions about visibility. Information privacy skeptics have argued that the information conveyed by most individual items of personal data is too banal to trigger privacy interests. They have asserted, further, that privacy interests cannot attach to information voluntarily made "visible" as part of an otherwise consensual transaction.

Under the influence of the information privacy law project, privacy discourse has changed. Many new legal and philosophical theories of privacy are organized explicitly around problems of information privacy and "privacy in public." Some scholars assert a "constitutive" relationship between flows of personal information and self-development.[6] Helen Nissenbaum argues that the collection and aggregation of personal information disrupts expectations of "contextual integrity" by allowing presence, appearance, and behavior in different contexts to be juxtaposed.[7] Drawing upon pragmatist philosophy and phenomenology, Daniel Solove argues that "digital dossiers" threaten a varied but related set of interests that are grounded in the logic of everyday experience.[8]

These theories suggest that the persistent theme of visibility in privacy discourse is a distraction from the more fundamental problem of informational accessibility. Although the theories differ from each other in important respects, an implicit premise of all of them is that databases and personal profiles can communicate as much or more than images. To the extent that privacy is conceived as encompassing a more general interest against accessibility, the adage that "a picture is worth a thousand words" requires rethinking. Visibility is an important determinant of accessibility, but threats to privacy from visual surveillance become most acute when visual surveillance and data-based surveillance are integrated, enabling both real-time identifica-

---

5 See, for example, *Kyllo v United States*, 533 US 27, 29 (2001); *California v Greenwood*, 486 US 35, 40–41 (1988). See also *R v Tessling*, [2004] 3 SCR 432, 434 (Can). *Kyllo* was thought to be a hard case precisely because it seemed to lie on the boundary between the two categories.

6 See, for example, Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 Stan L Rev 1373, 1424–25 (2000); Paul M. Schwartz, *Internet Privacy and the State*, 32 Conn L Rev 815, 856–57 (2000). See also Luciano Floridi, *The Ontological Interpretation of Informational Privacy*, 7 Ethics & Info Tech 185, 194–99 (2005).

7 See generally Helen Nissenbaum, *Privacy as Contextual Integrity*, 79 Wash L Rev 119 (2004). See also generally Jeffrey Rosen, *The Unwanted Gaze: The Destruction of Privacy in America* (Random House 2000).

8 See generally Daniel J. Solove, *Conceptualizing Privacy*, 90 Cal L Rev 1087 (2002).

tion of visual surveillance subjects and subsequent searches of stored visual and databased surveillance records. And, for the most part, informational accessibility does not result from a conscious decision to target particular individuals. Rather, accessibility is embedded in the design of social and technical institutions.[9]

Even as information privacy theorists have sought to shift the focus of the discussion about privacy interests, however, the terms of both academic and public debate continue to return inexorably to visibility, and more particularly to an understanding of surveillance as direct visual observation by centralized authority figures. Within popular privacy discourse, this metaphoric mapping tends to be organized around the anthropomorphic figure of Big Brother. Academic privacy theorists have tended to favor the motif of the Panopticon, a model prison proposed by Jeremy Bentham that consists of cells concentrically arranged around a central guard tower, from which the prison authority might see but not be seen.[10] Historically and also etymologically, the Panopticon suggests that direct visual observation by a centralized authority is both the most effective means and the best exemplar of surveillance for social control.

It is not particularly surprising that the paradigm cases of privacy invasion should be conceptualized in terms of sight. The cultural importance of visibility extends well beyond privacy law, and well beyond law more generally. Within Western culture, vision is linked metaphorically with both knowledge and power. The eye has served throughout history as a symbol of both secular and religious authority. The Judeo-Christian God is described as all-seeing, and worldly leaders as exercising "oversight" or "supervision."[11] Cartesian philosophy of mind posits that objects and ideas exist in the "unclouded" mind, where truth is revealed by the "light of reason."[12] In the language of

---

9 See, for example, Daniel J. Solove, *The Digital Person: Technology and Privacy in the Information Age* 97–101 (NYU 2004); Richards, 94 Georgetown L J at 1095–1102 (cited in note 1); Schwartz, 32 Conn L Rev at 831 (cited in note 6), citing Joel R. Reidenberg, *Lex Informatica: The Formulation of Information Policy Rules through Technology*, 76 Tex L Rev 553, 556 (1998).

10 See, for example, Sonia K. Katyal, *The New Surveillance*, 54 Case W Res L Rev 297, 317–19 (2003); Rosen, *The Unwanted Gaze* at 213–14 (cited in note 7); Schwartz, 32 Conn L Rev at 852–53 (cited in note 6). See also Michel Foucault, *Discipline and Punish: The Birth of the Prison* 195–209 (Vintage 1977) (Alan Sheridan, trans) (describing the Panopticon).

11 The Hebrew Bible refers to God in a number of ways, including *El-Roi*, or "God who sees." See, for example, Genesis 16:13. The all-seeing God figures prominently in the religious iconography of the Renaissance, and the linkages between vision, power, and knowledge continue in the subsequent secular iconography of the Enlightenment. See Astrit Schmidt-Burkhardt, *The All-Seer: God's Eye as Proto-surveillance*, in Thomas Y. Levin, Ursula Frohne, and Peter Weibel, eds, *Ctrl [Space]: Rhetorics of Surveillance from Bentham to Big Brother* 17, 18–26 (MIT 2002).

12 See Rene Descartes, *Rules for the Direction of the Mind*, in 31 *Great Books of the Western World* 4 (Encyclopædia Britannica 1952) (Elizabeth S. Haldane and G.R.T. Ross, trans). See

everyday conversation, someone who understands is one who "sees"; someone who doesn't get it is "blind." Claims of privacy invasion are claims about unwanted subjection to the knowledge or power of others. Within this metaphoric framework, it makes sense for such claims to be conceptualized in terms of seeing and being seen.

Yet this way of understanding privacy carries significant intellectual and political costs. If it makes sense to conceptualize privacy problems in terms of visibility, it also makes sense to conclude that problems that cannot be so conceptualized are not privacy problems. As Solove observes, identifying privacy problems becomes analytically more difficult when there is no single Big Brother at which to point.[13] Privacy doubters, meanwhile, often cannot get past the ways in which the practices that privacy advocates seek to challenge fail to align with the dominant metaphors. But knowledge, power, and sight are not the same. If "privacy" really is meant to denote an effective barrier to knowledge or the exercise of power by others, equating privacy invasion with visibility assumes what ought to be carefully considered.

Work within the emerging field of surveillance studies calls into question the implicit linkages between surveillance, visual observation, and centralization that the conventional metaphors for privacy invasion have tended to reinforce. Scholars in this field have brought a variety of allied disciplines—including sociology, urban geography, communications theory, and cultural studies—to bear on the institutions and subjects of surveillance. This work enables a richer understanding of how surveillance functions, and of what "privacy" interests might include.

Much work in surveillance studies builds upon Michel Foucault's landmark study of the prison and its role in the emergence of modern techniques of social discipline.[14] US privacy theorists have drawn on this work primarily for its discussion of Bentham's Panopticon, but have tended not to notice that Foucault offered the Panopticon as a metaphor for a different and more comprehensive sort of discipline that is concerned more fundamentally with classification and normalization.[15] One of his central insights was that in modern societies social discipline is accomplished by statistical methods. "[W]hereas the ju-

---

also George Lakoff and Mark Johnson, *Philosophy in the Flesh: The Embodied Mind and Its Challenge to Western Thought* 393–96 (Basic Books 1999). According to Bernard Hibbitts, the cultural preeminence of sight is linked to the spread of literacy, and reached its zenith with the development of Cartesian rationalism. Bernard J. Hibbitts, *Making Sense of Metaphors: Visuality, Aurality, and the Reconfiguration of American Legal Discourse*, 16 Cardozo L Rev 229, 244–61 (1994).

13 See Solove, *The Digital Person* at 33–35 (cited in note 9).

14 See generally Foucault, *Discipline and Punish* (cited in note 10).

15 See id at 205–06. The exception is James Boyle, *Foucault in Cyberspace: Surveillance, Sovereignty, and Hardwired Censors*, 66 U Cin L Rev 177, 184–88 (1997).

ridical systems define juridical subjects according to universal norms, the disciplines characterize, classify, specialize; they distribute along a scale, around a norm, hierarchize individuals in relation to one another and, if necessary, disqualify and invalidate."[16] This process does not require a centralized authority; instead, it is most powerful when it is most widely dispersed among the civil and private institutions that regulate everyday life.[17] These observations, which have obvious application to a wide variety of statistical and actuarial practices performed in both government and private sectors, have served as the foundation for elaboration of the work of modern "surveillance societies."[18]

Surveillance in the panoptic sense thus functions both descriptively and normatively. It does not simply render personal information *accessible* but rather seeks to render individual behaviors and preferences *transparent* by conforming them to preexisting frameworks. And in seeking to mold the future, surveillance also shapes the past: by creating fixed records of presence, appearance, and behavior, surveillance constitutes institutional and social memory.[19]

Some surveillance theorists argue that surveillance in postindustrial, digitally networked societies is even more radically decentralized and resilient than Foucault's work suggests. Building on Gilles Deleuze and Félix Guattari's work on systems of social control,[20] Kevin Haggerty and Richard Ericson argue that the prevailing modality of surveillance is the "surveillant assemblage": a heterogeneous, loosely coupled set of institutions that seek to harness the raw power of information by fixing flows of information cognitively and spatially.[21] Surveillant assemblages grow rhizomatically, "across a series of interconnected roots which throw up shoots in different locations," and for this reason they are extraordinarily resistant to localized disruption.[22] Of critical importance, the surveillant assemblage operates

16 Foucault, *Discipline and Punish* at 223 (cited in note 10).

17 Id at 207–17, 222–27.

18 See David Lyon, *Surveillance Society: Monitoring Everyday Life* 33–35, 114–18 (Open University 2001); Oscar H. Gandy, Jr., *The Panoptic Sort: A Political Economy of Personal Information* 15–52 (Westview 1993). See generally David Murakami Wood, ed, *Surveillance Studies Network, A Report on the Surveillance Society* (Mark Siddoway/Knowledge House 2006); Kirstie Ball, *Elements of Surveillance: A New Framework and Future Directions*, 5 Info Commun & Socy 573 (2002).

19 See Michael R. Curry and Leah A. Lievrouw, *Places to Read Anonymously: The Ecology on Attention and Forgetting* 5 (working paper, 2004), online at http://www.spatial.maine.edu/~nittel/lp/curry-lievrouw_paper.pdf (visited Jan 12, 2008), quoting Jean-François Blanchette and Deborah G. Johnson, *Data Retention and the Panoptic Society: The Social Benefits of Forgetfulness*, 18 Info Socy 33, 35 (2002).

20 Gilles Deleuze and Félix Guattari, *A Thousand Plateaus: Capitalism and Schizophrenia* (Minnesota 1987) (Brian Massumi, trans).

21 Kevin D. Haggerty and Richard V. Ericson, *The Surveillant Assemblage*, 51 Brit J Sociology 605, 605 (2000).

22 Id at 614.

upon its subjects not only by the "normalized soul training" of Foucauldian theory, but also by seduction.[23] Flows of information within the surveillant assemblage promise a cornucopia of benefits and pleasures, including price discounts, social status, and voyeuristic entertainment. In return, the surveillant assemblage demands full enrollment.

An alternative approach to surveillance studies uses performance theory to interrogate the effects of networked databases on the performance of identity. Performance theory melds the methodologies of speech act theory, which emphasizes the performative force of utterances; cultural anthropology, which describes culture as arising through performance; and deconstruction, which regards language as encoding multiple texts rather than universal truths.[24] Performance theorists argue that "identity" is neither fixed nor unitary, but rather is constituted by performances that are directed at different audiences.[25] From this perspective, the problem with surveillance is that it seeks to constitute individuals as fixed texts upon which invariant meanings can be imposed.[26] The struggle for privacy is recast as the individual's effort to assert multiplicity and resist "norming." This account emphasizes agency to a far greater degree than the Foucauldian and Deleuzian accounts. It too is concerned with normalization and transparency, but it argues that human nature is much more impervious to normalization and transparency than those literatures suggest, and that the subjects of surveillance are knowing and only partially compliant participants in their own seduction.

Unlike their European and Canadian counterparts, US privacy theorists generally have resisted making these connections between transparency, normalization, seduction, and fixity of meaning. Some US privacy theorists have argued that the collection and aggregation of personal information is harmful because it creates the potential for

---

23 Id at 615–16.

24 Canonical works in these fields include J.L. Austin, *How to Do Things with Words* (Harvard 1962); Clifford Geertz, *Thick Description: Toward an Interpretive Theory of Culture*, in *The Interpretation of Cultures* 3 (Basic 1973); Erving Goffman, *The Presentation of Self in Everyday Life* (Doubleday Anchor 1959); Jacques Derrida, *Signature Event Context*, in *Margins of Philosophy* 307 (Chicago 1982) (Alan Bass, trans).

25 See, for example, Andrew Parker and Eve Kosofsky Sedgwick, *Introduction*, in Andrew Parker and Eve Kosofsky Sedgwick, eds, *Performativity and Performance* 1, 6–8 (Routledge 1995); Judith Butler, *Gender Trouble: Feminism and the Subversion of Identity* 24–25 (Routledge 1990).

26 See David J. Phillips, *From Privacy to Visibility: Context, Identity, and Power in Ubiquitous Computing Environments*, 23 Soc Text 95, 101 (2005); John E. McGrath, *Loving Big Brother: Performance, Privacy and Surveillance Space* 12–14 (Routledge 2004); Hille Koskela, *Webcams, TV Shows, and Mobile Phones: Empowering Exhibitionism*, 2 Surveillance & Socy 199, 206 (2004); Stan Karas, *Privacy, Identity, Databases*, 52 Am U L Rev 393, 417–24 (2002).

hasty and erroneous judgments.[27] That argument seems to presume the existence of a fixed self defined by a set of invariant, theoretically accessible truths; it suggests that the problem with profiling is its inevitable, unacceptably high rate of error. Antidiscrimination theorists have focused on the ways in which profiling intersects with harmful stereotypes about minority groups, but have tended to resist generalizing that insight to profiling and normalization more generally.[28] Surveillance theorists, in contrast, argue that the logics of transparency and discrimination are inseparable.[29] They also identify a more fundamental inequality embedded in the logic of informational transparency. The transparency sought by surveillance runs only one way; it does not extend to the algorithms and benchmarks by which *all* individuals in surveillance societies are categorized and sorted.

US privacy scholars' resistance to the theoretical approaches employed by surveillance studies scholars also is not especially surprising, as it is rooted in core commitments—to individual autonomy and to the possibility of value-neutral knowledge of human nature—that derive from the tradition of liberal political economy within which US legal academics are primarily trained. Those commitments tend to foreclose other approaches that emphasize the mutually constitutive interactions between self and culture, the social construction of systems of knowledge, and the interplay between systems of knowledge and systems of power. They therefore require rejection of the docile bodies of Foucauldian theory, the assimilated denizens of Deleuzian systems of social control, and the fragmentary, protean selves posited by performance theorists.

It is possible, however, to meld all three sets of insights about the function of surveillance with the more traditionally liberal concerns that have preoccupied US privacy theorists. One can choose to understand liberal political theory and Foucauldian poststructuralism as delineating irreconcilable opposites, or one can understand them as describing two (equally implausible) endpoints on a continuum along which social influence and individual liberty combine in varying proportions. As a counterpoint to the universalist aspirations of liberal political theory, Foucauldian theory seeks to cultivate a critical stance

---

27 See generally Rosen, *The Unwanted Gaze* (cited in note 7); Daniel J. Solove, *The Virtues of Knowing Less: Justifying Privacy Protections against Disclosure*, 53 Duke L J 967 (2003).

28 See, for example, Frederick Schauer, *Profiles, Probabilities, and Stereotypes* 22 (Belknap 2003); Deborah Hellman, *The Expressive Dimension of Equal Protection*, 85 Minn L Rev 1 (2000); David Cole, *No Equal Justice: Race and Class in the American Criminal Justice System* 16–27 (New Press 1999).

29 See, for example, Oscar Gandy, Jr., *Data Mining, Surveillance, and Discrimination in the Post-9/11 Environment*, in Kevin D. Haggerty and Richard V. Ericson, eds, *The New Politics of Surveillance and Visibility* 363, 363–64 (Toronto 2006).

toward claims to knowledge.[30] Performance theory takes background social shaping for granted and focuses on the range of motion that it affords for the process of self-articulation through experimentation and play. Haggerty and Ericson's theory of the surveillant assemblage, meanwhile, seeks to cultivate a subtler appreciation of the affective dimensions of social control. In a society committed at least to the desirability of the liberal ideal of self-determination, these perspectives on surveillance are important. In such a society, pervasive transparency is troubling because it constrains the range of motion for the development of subjectivity through both criticism and performance, and it does not automatically cease to be troubling when the subjects of surveillance have indicated their willing surrender.

This account of the relation between informational transparency and subjectivity is attractive, moreover, because it offers a useful perspective on philosophical differences among US legal theorists and philosophers about the ultimate value of privacy. Some theorists have asserted that privacy serves principally instrumental values, while others are adamant in linking privacy deontologically to care for the (liberal) self. Privacy performs both functions. Choices about the permissible extent and nature of surveillance are choices about the scope for self-articulation; in a very real sense, they are what enable or disable pursuit of the ideal that the liberal self represents. For precisely that reason, they are also choices about the definition and articulation of collective identity.

The account of privacy as relative informational opacity runs into difficulty, however, when we return to the problem of visual surveillance in public places. In particular, an informational transparency framework for conceptualizing privacy harms suggests that purely localized visual surveillance is relatively innocuous. The real danger to privacy comes from databases; visual surveillance creates pressing privacy threats only when it is digital, networked, and combined with other sources of information. Yet the theory doesn't align with the practice: surveillance cameras produce effects that are experienced by real people as altering levels of experienced privacy. This suggests that the informational transparency framework is incomplete.

II. VISIBILITY AND EXPOSURE

Linking privacy to informational transparency tends to mask a conceptually distinct privacy harm that is spatial, and concerns the

30 Consider Bernard E. Harcourt, *An Answer to the Question: "What Is Poststructuralism?,"* (Chicago Public Law and Legal Theory Working Paper No 156, Mar 2007), online at http://ssrn.com/abstract=970348 (visited Jan 12, 2008).

nature of the spaces constituted by and for pervasive, continuous observation. Those spaces are characterized by what I will call a condition of exposure. The term "condition" is intended to signify that exposure is not a given but rather a design principle that in turn constrains the range of available behaviors and norms. Neither privacy law nor privacy theory has recognized an interest in limiting exposure uncoupled from the generally acknowledged interest in limiting observation, and in general we lack a vocabulary for conceptualizing and evaluating such an interest.

Since the US legal system purports to recognize an interest in spatial privacy, it is useful to begin there. Doctrinally, whether surveillance invades a legally recognized interest in spatial privacy depends in the first instance on background rules of property ownership. Generally speaking, surveillance is fair game within public space, and also within spaces owned by third parties, but not within spaces owned by the targets of surveillance. Those baseline rules, however, do not invariably determine the outcomes of privacy disputes. Expectations deemed objectively reasonable can trump the rules that otherwise would apply in a particular space. Thus, for example, a residential tenant is entitled to protection against direct visual observation by the landlord even though she does not own the premises,[31] and a homeowner is not necessarily entitled to protection against direct visual observation by airplane overflight,[32] nor to privacy in items left out for garbage collection.[33] Employees sometimes can assert privacy interests against undisclosed workplace surveillance.[34]

For purposes of this essay, the interesting thing about the reasonable expectations test is that it is fundamentally concerned not with expectations about the nature of particular *spaces*, but rather with expectations about the accessibility of *information* about activities taking place in those spaces. Even the exceptions prove the rule: *Kyllo v United States*,[35] styled as a ringing reaffirmation of the traditional privacy interest in the home, in fact upholds that interest only against information-gathering technologies "not in general public use."[36] Similarly, although legal scholars disagree about the precise nature of the privacy interest, they seem to agree that cognizable injury would re-

31 See *Hamberger v Eastman*, 206 A2d 239, 242 (NH 1964). See also *Chapman v United States*, 365 US 610, 616–17 (1961).

32 See *Florida v Riley*, 488 US 445, 451 (1989); *California v Ciraolo*, 476 US 207, 214–15 (1986).

33 See *California v Greenwood*, 486 US 35, 40 (1988).

34 See *O'Connor v Ortega*, 480 US 709, 713–14 (1987); *Mancusi v DeForte*, 392 US 364, 369 (1968).

35 533 US 27 (2001).

36 Id at 34.

quire the involvement of a human observer who perceives or receives information.[37] Focusing on the accessibility of information also explains why no privacy interest attaches to most activities in public spaces and nonresidential spaces owned by third parties: persons who voluntarily enter such premises have impliedly consented to being seen there.

In short, and paradoxically, prevailing legal understandings of spatial privacy do not recognize a harm that is distinctively spatial: that flows from the ways in which surveillance, whether visual or data-based, alters the spaces and places of everyday life. The information privacy law project has tended to ratify this omission, precisely because its primary interest has been information rather than the bodies and spaces to which it pertains. Many information privacy theorists criticize spatial metaphors in privacy discourse, arguing that they muddy rigorous analysis of privacy issues in the information age.[38] And this resistance too is rooted in the tradition of liberal political economy, which for the most part does not consider concrete, particular bodies and spaces at all.

Yet resistance to spatialization in privacy theory leaves important dimensions of the experience of surveillance unexplained. Consider an individual who is reading a newspaper at a plaza café in front of a downtown office building. The building's owner has installed surveillance cameras that monitor the plaza on a twenty-four-hour basis. Let's assume the cameras in this example are clearly visible, and clearly low-tech and analog. It would be reasonable for the individual to assume that they probably are not connected to anything other than the building's own private security system. Most likely, tapes are stored for a short period of time and then reused. The consensus view in US privacy theory tends to be that there is essentially no legitimate expectation of privacy under these circumstances, and that the surveillance therefore should not trouble us. But those surveilled often feel quite differently. Even localized, uncoordinated surveillance may be experienced as intrusive in ways that have nothing to do with whether data trails are captured.[39] Or consider the ways in which spatial meta-

---

37 See, for example, Rosen, *The Unwanted Gaze* at 8 (cited in note 7); Lisa Austin, *Privacy and the Question of Technology*, 22 Law & Phil 119, 126 (2003); Ruth Gavison, *Privacy and the Limits of Law*, 89 Yale L J 421, 432 (1980) ("[A]ttention alone will cause a loss of privacy even if no new information becomes known.").

38 See, for example, Solove, 90 Cal L Rev at 1094–95, 1151 (cited in note 8); Lloyd L. Weinreb, *The Right to Privacy*, in Ellen Frankel Paul, Fred D. Miller, Jr., and Jeffrey Paul, eds, *The Right to Privacy* 25, 26–27 (Cambridge 2000). The exception is Helen Nissenbaum, who does not criticize spatialization and whose "contextual integrity" framework for privacy accommodates spatial privacy interests. See Nissenbaum, 79 Wash L Rev at 137–42 (cited in note 7).

39 See generally Don Mitchell, *The Right to the City: Social Justice and the Fight for Public Space* (Guilford 2003). See also Marc Jonathan Blitz, *Video Surveillance and the Constitution of*

phors continually recur in discussions of privacy. Even in contexts that are not thought to involve spatial privacy at all, judges and scholars repeatedly refer to "spheres" and "zones" to describe the privacy that the law should attempt to guarantee.[40]

Because information-based analytical frameworks don't recognize these dimensions of the spatial privacy interest, commentators operating within those frameworks tend to question whether they are "real." Yet that conclusion denies the logic of embodied, situated experience. Surveillance infrastructures alter the experience of places in ways that do not depend entirely on whether anyone is actually watching. Governments know this well; that is part of the point of deploying surveillance infrastructures within public spaces. It seems sounder to conclude that the information-based frameworks are incomplete. Conceptualizing the privacy interest as having an independently significant spatial dimension explains aspects of surveillance that neither visibility nor informational transparency can explain.

Work in surveillance studies suggests that direct visual surveillance affects the experience of space and place in two ways that an emphasis on informational transparency doesn't completely capture. First, surveillance fosters a kind of passivity that is best described as a ceding of power over space. As geographer Hille Koskela puts it, visual surveillance constitutes "space as a container" for passive objects.[41] She distinguishes the spatial shaping that produces "container-space" from the "power-space" constituted by panoptic strategies of normalization, which depend on access to particularized information. But the "containerization" of space is itself a panoptic strategy. Panopticism in the Foucauldian sense is both statistical and architectural; it entails ordering of spaces to obviate the need for continual surveillance and to instill tractability in those who enter.[42] Our newspaper-reading individual cannot see whether anyone is watching her, but she can see that the plaza has been re-architected to allow observation secretly and at will, and that there is no obvious source of information about the surveillance and no evident method of recourse if she wishes to lodge a

Public Space: Fitting the Fourth Amendment to a World That Tracks Image and Identity, 82 Tex L Rev 1349, 1374–98 (2004).

40 See, for example, *Zablocki v Redhail*, 434 US 374, 397 n 1 (1978) (Powell concurring) (observing that the Court's prior decisions establish a "sphere of privacy or autonomy" within the marital relationship); *Griswold v Connecticut*, 381 US 479, 485 (1965) (describing a "zone of privacy created by several fundamental constitutional guarantees"); *Dietemann v Time, Inc*, 449 F2d 245, 248–49 (9th Cir 1971).

41 Hille Koskela, *"The Gaze without Eyes": Video-surveillance and the Changing Nature of Urban Space*, 24 Progress in Hum Geography 243, 250 (2000).

42 See Foucault, *Discipline and Punish* at 206 (cited in note 10); Julie E. Cohen, *Pervasively Distributed Copyright Enforcement*, 95 Georgetown L J 1, 23 (2006).

complaint. In Hohfeldian terms,[43] the reconfiguration places individuals under a twofold disability: the targets of surveillance cannot entirely avoid the gaze (except by avoiding the place) and also cannot identify the watchers. We can say, therefore, that surveillance alters the balance of powers and disabilities that obtains in public places. It instills an expectation of being surveilled, and contrary to the conventional legal wisdom, this reasonable expectation and the passivity that it instills are precisely the problem.

Performance theory reminds us that individuals surveilled are not only passive bodies, and this leads us to the second way in which surveillance affects the experience of space and place. Like identities, places are dynamic and relational; they are constructed over time through everyday practice.[44] Surveillance alters important parameters of both processes. Building on work in feminist geography, Koskela argues that surveillance alters a sense of space that she calls "emotional space." She observes that "[t]o be under surveillance is an ambivalent emotional event. A surveillance camera ... can at the same time represent safety and danger."[45] This point contrasts usefully with US privacy theorists' comparatively single-minded focus on the "chilling effect"; it reminds us that surveillance changes the affective dimension of space in ways that that formulation doesn't address. Marc Augé has argued that the defining feature of contemporary geography is the "non-place."[46] Places are historical and relational; non-places exist in the present and are characterized by a sense of temporariness, openness, and solitariness.[47] Augé does not discuss surveillance, but the distinction between places and non-places maps well to the affective dimension of space that Koskela identifies. Augé's critics observe that "placeness" is a matter of perspective; for example, airports may be places to those who work there, while wealthy residential enclaves may be non-places to those whose entry incites automatic suspicion.[48] It may be most accurate to conceptualize "placeness" both as a matter of degree and as an attribute that may be experienced differently by different groups. Along this continuum, surveillance makes places

---

43 See Wesley Newcomb Hohfeld, *Fundamental Legal Conceptions as Applied in Judicial Reasoning and Other Legal Essays* 35–64 (Yale 1919) (Walter Wheeler Cook, ed).

44 See generally Henri Lefebvre, *The Production of Space* (Blackwell 1991) (Donald Nicholson-Smith, trans).

45 Koskela, 24 Progress in Hum Geography at 257 (cited in note 41).

46 See Marc Augé, *Non-places: Introduction to an Anthropology of Supermodernity* 75–115 (Verso 1995) (John Howe, trans).

47 Id at 77–86.

48 See generally Peter Merriman, *Driving Places: Marc Augé, Non-places, and the Geographies of England's M1 Motorway*, 21 Theory, Culture, & Socy 145 (2004).

more like non-places. Spaces exposed by surveillance function differently than spaces that are not so exposed.

I will characterize the spatial dimension of the privacy interest as an interest in avoiding or selectively controlling the conditions of exposure. This terminology is intended to move the discussion beyond both visibility and transparency to capture the linked effects of architecture and power as experienced by embodied, situated subjects. With respect to space, surveillance employs a twofold dynamic of containerization and constraint to pursue large-scale behavioral modification. Koskela observes that surveillance makes public spaces less predictable for the watched.[49] The relation is reciprocal: surveillance also attempts to make those spaces more predictable for the watchers. By altering the balance of powers and disabilities, exposure changes the parameters that shape the ongoing performance of identity, community, and place.

The effects of exposure and transparency are complementary, and the genius of surveillance appears most clearly when one considers them together. Transparency alters the parameters of evolving subjectivity; exposure alters the capacity of places to function as contexts within which identity is developed and performed. Surveillance directed at transparency seeks to systematize, predict, and channel difference; surveillance directed at exposure seeks to prevent unsystematized, unpredictable difference from emerging.

III. EXPOSURE ONLINE

This understanding of the spatial dimension of privacy is relevant not only to physical spaces, but also to the ongoing debate about privacy interests in online conduct. The mismatch between online conduct and fixed physical place is one of the principal reasons that privacy theorists have offered to support a purely information-based definition of privacy interests. Privacy skeptics, meanwhile, assert that whether or not online forums correspond to physical places, online conduct that is visible to others is not private in any meaningful sense. Both arguments overlook the extent to which online conduct and online surveillance are experienced spatially.

Let us now zoom in on our café-sitting individual as she uses her laptop computer to explore the web, view and download "content," write pseudonymous blog posts, and send email. Privacy rules derived from ownership and expectation suggest that she can have no legally cognizable expectation of privacy in most of these activities. The software is licensed, the communications networks are owned by third

49 Koskela, 24 Progress in Hum Geography at 250 (cited in note 41).

parties, and it is increasingly common knowledge that online activities are potentially subject to pervasive surveillance by governments and commercial interests. Federal statutes carve out limited zones of privacy, but as their definitional frameworks are challenged by rapid technological change, those statutes more often serve to highlight the absence of a generally applicable privacy interest in online activity.

Here again, the reasonable expectation standard begs the question: when does surveillance of online activities change expectations in a way that we as a society should find objectionable? As the hypothetical suggests, the question cannot be answered simply by invoking an expanded conception of the privacy of the home. Information privacy theorists have objected, rightly, that this move tethers spatial privacy interests to a fixed physical space and ignores the fact that many online activities occur outside the home. A privacy analysis for the information age must focus on something other than physical location.

The question also cannot be answered by reifying communications networks as separate "spaces." Online "space" is not separate from "real" space. Communications networks are layered over and throughout real space, producing a social space that in totality is more accurately understood as networked space.[50] Actions taken in physical space have important consequences online, and vice versa. In ways that "real" space does not, online "space" contains material traces of intellectual, emotional, and relational movement, but privacy law and policy must be crafted for those who live in the real world.

A viable theory of privacy for the networked information age must consider the extent to which the "privacy of the home" has served as a sort of cultural shorthand for a broader privacy interest against exposure. The home affords a freedom of movement that is both literal and metaphorical, and that has physical, intellectual, and emotional dimensions: we can move from room to room, we can speak our minds and read whatever interests us, we can pursue intimacy in relationships. The advent of networked space challenges privacy theorists to articulate a more general account of the spatial entailments of intellectual, emotional, and relational activities. By analogy to the home, we might envision a zone of personal space that permits (degrees of) unconstrained, unobserved physical and intellectual movement. That zone furnishes room for a critical, playful subjectivity to develop. This account of spatial privacy matches the experience of privacy in ways that the purely informational conception does not.

When the spatial dimension of privacy is understood in this way, it becomes easier to see that surveillance of online activities alters the

50 See Julie E. Cohen, *Cyberspace as/and Space*, 107 Colum L Rev 210, 235–48 (2007).

experience of space in the same ways that surveillance of "real" places does. From the standpoint of Foucauldian theory, surveillance of online activities is a logical extension of the panoptic gaze, and not only for purposes of imposing transparency and normalization. To be most effective, the "containerization" of space must extend to intellectual, emotional, and relational processes conducted online. From the standpoint of Deleuzian theory, surveillance of online activities furthers the goals of the surveillant assemblage; it hastens the conversion of bodies and behaviors into flows of data.[51] As in physical space, exposure of activities in networked space alters the affective dimension of online conduct. That process in turn affects the ongoing construction of self, place, and community not only on the network, but within networked space more generally.

Other social and technological changes also can alter the balance of powers and disabilities that exists in networked space. Imagine now that our café-sitting individual engages in some embarrassing and unsavory behavior—perhaps she throws her used paper cup and napkin into the bushes, or coughs on the milk dispenser. Another patron of the café photographs her with his mobile phone and posts the photographs to an internet site dedicated to shaming the behavior.[52] This example reminds us that being in public entails a degree of exposure, and that (like informational transparency) sometimes exposure can have beneficial consequences.[53] Maybe we don't want people to litter or spread germs, or to drive aggressively,[54] and if the potential for exposure reduces the incidence of those behaviors, so much the better. Or suppose our café-sitter posts her own location to an internet site that lets its members log their whereabouts and activities.[55] This example reminds us that exposure may be desired and eagerly pursued; in such cases, worries about privacy seem entirely off the mark. But the problem of exposure in networked space is more complicated than these examples suggest.

The sort of conduct in the first example, which antisurveillance activist Steve Mann calls "coveillance," figures prominently in two different claims about diminished expectations of privacy in public. Privacy critics argue that when technologies for surveillance are in

---

51 See Haggerty and Ericson, 51 Brit J Sociology at 608–09 (cited in note 21).

52 See, for example, HollaBackNYC, online at http://hollabacknyc.blogspot.com (visited Jan 12, 2008); How Drunk Am I?, online at http://www.howdrunkami.com (visited Jan 12, 2008). See also Kevin Werbach, *Sensors and Sensibilities*, 28 Cardozo L Rev 2321, 2325–29 (2007).

53 It also reminds us that online "space" and "real" space are not separate.

54 See generally Lior Jacob Strahilevitz, *"How's My Driving?" for Everyone (and Everything?)*, 81 NYU L Rev 1699 (2006).

55 See, for example, Twitter, online at http://www.twitter.com (visited Jan 12, 2008).

common use, their availability can eliminate expectations of privacy that might previously have existed. Mann argues that because coveillance involves observation by equals, it avoids the troubling political implications of surveillance.[56] But if the café-sitter's photograph had been posted to a site that collects photographs of "hot chicks," many women would understand the photographer's conduct as an act of subordination.[57] And there is more than an element of bootstrapping to the argument that coveillance eliminates expectations of privacy vis-à-vis surveillance. This is so whether or not one accepts the argument that coveillance and surveillance are meaningfully different. If they are different, then coveillance doesn't justify or excuse the exercise of power that surveillance represents. If they are the same, then the interest against exposure applies equally to both.

In practice, the relation between surveillance and coveillance is more mutually constituting than either of these arguments acknowledges. Many employers now routinely search the internet for information about prospective hires, so what began as "ordinary" coveillance can become the basis for a probabilistic judgment about attributes, abilities, and aptitudes. At other times, public authorities seek to harness the distributed power of coveillance for their own purposes—for example, by requesting identification of people photographed at protest rallies.[58] Here what began as surveillance becomes an exercise of distributed moral and political power, but it is power called forth for a particular purpose.

The relation between surveillance and self-exposure is similarly complex. Exposure is a critical enabler of interpersonal association; indeed, some feminist theorists argue that we are constituted predominantly by our relationships.[59] From this perspective, the argument that privacy functions principally to enable interpersonal intimacy gets it only half right.[60] Intimate relationships, community relationships,

---

56 Steve Mann, Jason Nolan, and Barry Wellman, *Sousveillance: Inventing and Using Wearable Computing Devices for Data Collection in Surveillance Environments*, 1 Surveillance & Socy 331, 348 (2003).

57 See Ellen Nakashima, *Harsh Words Die Hard on the Web; Law Students Feel Lasting Effects of Anonymous Attacks*, Wash Post A01 (Mar 7, 2007); Jill Filipovic, *Hi, I'm Jill, and Scummy Law School Sleazebags Have Gone after Me, Too*, Feministe (Mar 7, 2007), online at http://www.feministe.us/ blog/archives/2007/03/07/wapo-calls-out-law-school-pervs (visited Jan 12, 2008).

58 See Wayne Harrison, *CU Posts Pictures of Pot-smoking Event: Reward Offered for Information about People in Photos*, ABC 7 News Online (Apr 28, 2006), online at http://www.thedenverchannel.com/news/9063737/detail.html (visited Jan 12, 2008); Texas Border Watch, http://www.texasborderwatch.com (visited Jan 12, 2008).

59 See, for example, Jennifer Nedelsky, *Law, Boundaries, and the Bounded Self*, in Robert Post, ed, *Law and the Order of Culture* 162, 169 (California 1991).

60 See, for example, Julie C. Inness, *Privacy, Intimacy, and Isolation* 74–94 (Oxford 1992); Charles Fried, *Privacy*, 77 Yale L J 475, 484 (1968).

and more casual relationships all derive from *selective* exposure: from the ability to control in different ways and to differing extents what Erving Goffman called the "presentation of self."[61] It is this recognition that underlies the different levels of "privacy" enabled by some (though not all) social networking sites.[62] Scholars who study queer communities argue that exposure of matters conventionally considered "private" fulfills a similar function, enabling the formation of alternative communities constituted around challenges to conventional models of intimacy.[63] Surveillance changes the various dynamics of selective exposure, but the strand of surveillance studies literature affiliated with performance theory argues that exposure to surveillance can be similarly productive. Surveillance cameras can represent an invitation to perform in ways that transgress stated or implicit norms or exaggerate imputed characteristics; by the same token, self-exposure using networked information technologies can operate as resistance to narratives imposed by others.[64] The performative impulse introduces static into the circuits of the surveillant assemblage; it seeks to reclaim bodies and reappropriate spaces.

As this analysis suggests, interpreting self-exposure either as a blanket waiver of privacy or as an exercise in personal empowerment would be far too simple. Surveillance and self-exposure bleed into one another in the same ways that surveillance and coveillance do. As Jane Bailey and Ian Kerr demonstrate, and as millions of subscribers to social networking sites are now beginning to learn, the ability to control the terms of self-exposure in networked space is largely illusory: body images intended to assert feminist self-ownership are remixed as pornography, while revelations intended for particular social networks are accessed with relative ease by employers, police, and other authority figures.[65] Other scholars raise important questions about the origins of the desire for exposure. In an increasing number of contexts, the images generated by surveillance have fetish value. As Kirstie Ball puts it, surveillance creates a "political economy of interiority" organ-

---

61 See generally Goffman, *The Presentation of Self in Everyday Life* (cited in note 24); Irwin Altman, *The Environment and Social Behavior: Privacy, Personal Space, Territory, Crowding* (Brooks/Cole 1975).

62 See, for example, *Protect Your Privacy*, Facebook, online at http://www.facebook.com/sitetour/privacy.php (visited Jan 12, 2008).

63 See McGrath, *Loving Big Brother* at 61–62 (cited in note 26). See generally Michael Warner, *Publics and Counterpublics* (Zone Books 2002).

64 See McGrath, *Loving Big Brother* at 14–16 (cited in note 26); Koskela, *Webcams, TV Shows, and Mobile Phones* at 206–07 (cited in note 26).

65 Jane Bailey and Ian Kerr, *Seizing Control?: The Experience Capture Experiments of Ringley and Mann*, 9 Ethics & Info Tech 129, 132, 137 (2007).

ized around "the 'authenticity' of the captured experience."[66] Within this political economy, self-exposure "may represent patriotic or participative values to the individual,"[67] but it also may be a behavior called forth by surveillance and implicated in its informational and spatial logics.

These examples argue for more careful exploration of the individual and systemic consequences of exposure within networked space, however it is caused. While the law should not ignore changing social dynamics, it also should not overlook or oversimplify their causes and effects. Exposure online is a matter of concern for the same reasons that exposure in "real" space is; indeed, as the phenomenon of coveillance shows, the two cannot really be separated.

IV. TRANSPARENCY, EXPOSURE, AND PRIVACY SELF-DEFENSE

Finally, understanding privacy interests as including interests against both transparency and exposure raises questions about the efficacy of tools and practices for privacy self-defense. Modes of privacy self-defense directed solely at minimizing or equalizing visual or informational accessibility do not necessarily address the more general problems of transparency and exposure. Even if tools for privacy self-defense were designed with these more general problems in mind, it's not clear that the effort would succeed.

To see why, consider two general classes of privacy self-defense tools. The first consist of tools for "watching from below," or "sousveillance." A leading exponent of sousveillance is Mann, who employs wearable cameras to document visual surveillance in progress. When challenged by property managers or security personnel, he answers that the cameras are not under his direct control, and that it's up to his "controller" whether to turn them off. Mann envisions sousveillance as a species of situationist critique of surveillance: it is a way to "challenge and problematize both surveillance and acquiescence to it."[68]

As political performance art, sousveillance is brilliant. At times, however, Mann also appears to envision the condition of constant sousveillance as a normatively desirable way of living in the world. He contrasts the "reflectionism" of sousveillance with top-down privacy regulation, which he characterizes as a "pacifier," and argues that sousveillance emphasizes equality and participation.[69] That may be so, but sousveillance does not change the architectural conditions of sur-

---

66 Kirstie Ball, *Exposure: Exploring the Subject of Surveillance* 4–5 (unpublished manuscript, 2007).

67 Id at 1. See also Anita L. Allen, *Coercing Privacy*, 40 Wm & Mary L Rev 723, 743–45 (1999).

68 Mann, Nolan, and Wellman, 1 Surveillance & Socy at 332 (cited in note 56).

69 Id at 333, 345–47. See also David Brin, *The Transparent Society: Will Technology Force Us to Choose between Privacy and Freedom?* 3–26 (Addison-Wesley 1998).

veillance or the underlying inequalities that they reinforce. Nor does it challenge internalization of the condition of exposure; if anything, widespread sousveillance likely would produce the opposite effect.

The second general class of privacy self-defense tools consists of tools for hiding from surveillance. For example, portable Faraday cages can shield embedded radio-frequency identification (RFID) chips against external scanning.[70] Many privacy activists recommend that holders of RFID-embedded passports keep them in aluminum foil wrappers to prevent unauthorized capture of encoded personal information; one might do the same for one's EZ Pass transponder between transaction points. Other technologies enable anonymization of emails and blog posts; some privacy activists and entrepreneurs have envisioned anonymization becoming routine for a much broader range of online transactions and interactions.

These examples illustrate that hiding from surveillance can be easy in some contexts, but they also illustrate that even a robust commitment to hiding would be extraordinarily difficult for ordinary individuals to sustain in the face of routine practices of embedded computing that pervade networked space. One cannot escape the fact that the RFID transmitter must be removed from its protective coating in order to serve its intended purpose, which might be one that the individual wants or needs. At transaction points, the encoded information must be accessible, and at those locations the individual is exposed. Similarly, major commercial web sites generally are not configured to permit anonymous or robustly pseudonymous transactions. It is overwhelmingly likely that transaction points will continue to proliferate. For most people, the rewards of hiding won't outweigh the convenience of technologies like EZ Pass or the seduction of customer loyalty programs. Normatively speaking, it seems unfair to place responsibility for hiding on individuals when the deck is stacked so definitively against them.

Focusing on the spatial dimension of the privacy interest reminds us that hiding carries other costs as well, and not only those costs that are conventionally recognized. In "real" space, hiding generally is not considered a socially neutral activity. Unless it's Halloween or Mardi Gras, we tend to presume that people who wear masks in public are up to no good. But we presume this in part because a wide range of middle options—degrees of de facto anonymity and pseudonymity—has usually been available. Currently online spaces, like real spaces,

---

70 See *Faraday Cage*, SearchSecurity.com, (Information Security Magazine, Dec 21, 2003), online at http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci942282,00.html (visited Jan 12, 2008).

support a variety of norms regarding "nymity."[71] In some online spaces, nymity is the rule; in others, it occurs often enough to be unremarkable; in others, it is unimportant; in still others, it is perceived as creating risks that may threaten the community's reason for being. If forced or trivially easy identification became the norm, we might come to embrace more committed hiding in a broader range of circumstances. But, just as the nature of "real" space would change profoundly if everyone wore either a bar code or a mask, the feel of online spaces, and of networked space more generally, will change accordingly.

The lesson of these examples is not that privacy self-defense is a bad idea, but rather that privacy self-defense alone can't neutralize either the institutional predicates of transparency or the architectural predicates of exposure. Privacy self-defense operates at the individual level, while surveillance operates at the collective level. The informational and spatial logics of surveillance require a considered, collective response.

CONCLUSION

Within the discourse of privacy, the language of visibility both conceals and reveals. Understanding privacy as an interest against visibility/informational accessibility misses an important piece of the logic of informational transparency. The privacy interest against transparency encompasses not only the individualized information that surveillance collects, but also the informational frameworks that it imposes. Yet the problem of visual privacy also points us to dimensions of the privacy interest that a focus on privacy as relative informational opacity cannot explain. Privacy encompasses an interest in the structure of experienced space, and this interest is threatened under conditions of visual or informational exposure.

Both transparency and exposure are questions of degree; the law can't (and shouldn't) regulate every instance of either. But privacy law and theory should recognize them as independent harms, so that a conversation about possible responses can proceed.

---

[71] Ian Kerr and Alex Cameron, *Nymity, P2P, and ISPs: Lessons from* BMG Canada Inc. v. John Doe, in Katherine Strandburg and Daniela Stan Raicu, eds, *Privacy and Technologies of Identity: A Cross-disciplinary Conversation* 269, 271–72 (Springer 2006).