5
Privacy, Autonomy, and Information

In the last two decades, the environmental and social determinants of privacy have undergone rapid change. The amount of information collected about both individuals and social groups has grown exponentially and covers an astonishing range of subject matter, from purchasing history to browsing behavior to intellectual preferences to genetic predispositions. This information lasts longer and travels farther than ever before; it is stored in digital databases, exchanged in markets, and "mined" by both government and private actors for insights into individual and group behavior. The increase in data-processing activity coincides with the rapid spread of identity-linked authentication regimes for controlling access to spaces and resources, both real and digital. Authentication data are added to the other information stored in digital databases, creating comprehensive, persistent records of individual activity. The last two decades also have witnessed a dramatic upswing in real-time monitoring—by camera, satellite, and electronic pattern-recognition tools—of public spaces, privately owned spaces, and traffic across communications networks.

Government entities are involved in many of these activities, but the vast majority of data-mining, authentication, and monitoring initiatives do not originate with government. They originate in private-sector desires to learn more about current and prospective customers, to administer access to real and virtual resources, and to manage communication traffic over networks. Moreover, the increasingly widespread diffusion of cameras, networked personal devices, and social-networking platforms means that individuals and social groups themselves actively participate in many of these activities.

What all this signifies for people's understandings and expectations of privacy is hard to understand. Surveys report that ordinary people experience a relatively high generalized concern about privacy but a relatively low level of concern about the data generated by specific transactions, movements, and communications. Some policy makers interpret the surveys as indicating either a low commitment to privacy or a general readiness to trade privacy for other goods. Others argue that the various "markets" for privacy have informational and structural defects that prevent them from generating privacy-friendly choices. They argue, as well, that inconsistencies between reported preferences and revealed behavior reflect a combination of resignation and befuddlement; most Internet users do not understand how the technologies work, what privacy policies mean, or how the information generated about them will actually be used.[1]

Confronted with these developments and struggling to make sense of them, courts increasingly throw up their hands, concluding that constitutional guarantees of privacy simply do not speak to many of the new technologies, business models, and behaviors, and that privacy policy is best left to legislators. Legislators are quick to hold hearings but increasingly slow to take action; in many cases, they prefer to delegate day-to-day authority to regulators. Regulators, for their part, rely heavily on principles of notice, consent, reasonable expectation, and implied waiver to define the scope of individual rights with respect to the practices that fall within their jurisdiction.

Legal scholars also have struggled to respond to these social, technological, and legal trends. There is widespread (though not unanimous) scholarly consensus on the continuing importance of privacy in the networked information economy, but little consensus about what privacy is or should be. Among other things, legal scholars differ on whether privacy is a fundamental human right, what circumstances would justify pervasive government monitoring of movements and communications, whether guarantees of notice and informed consent are good or even effective safeguards against private-sector practices that implicate privacy, and what to make of the inconsistency between expressed preferences for more privacy and revealed behavior that suggests a relatively low level of concern.

Despite the voluminous amount of scholarship now being published on privacy issues, however, scholarly accounts of privacy within U.S. legal theory are incomplete in three ways that go to the most fundamental questions about what privacy interests encompass. First, privacy scholars generally have assumed that the self that privacy protects is characterized by its autonomy. This formulation does not withstand close scrutiny—scholars cannot agree on whether "autonomy" denotes an absolute condition or a matter of degree, and neither understanding makes sense taken on its own terms—and the policy recommendations it generates are incoherent. Yet privacy theory clings to it nonetheless. Privacy scholars have seemed both unable and unwilling to generate a different theory of the self that privacy protects. Second, although privacy theorists have articulated a variety of collective interests that privacy serves, they have avoided digging too close to the root of the asserted social interest in denying privacy—in gathering information, imposing identity-linked authentication procedures, and monitoring spaces and networks. Scholarly reluctance to confront the case against privacy weakens the case for privacy; collective-interest justifications that seem incomplete are more easily swept aside. Finally, privacy theory offers a very poor account of the metaphors used to describe privacy interests and harms. Most privacy theorists disdain spatial metaphors for privacy as ill-suited to the networked information age, but have not explored why spatial metaphors continually recur in privacy discourse or what that recurrence might mean for privacy law. At the same time, they have seemed not to notice the dominance of visual metaphors in privacy discourse, and have not considered the ways in which the implicit equation of privacy with invisibility structures the legal understanding of privacy interests and harms.

As in the case of copyright, the deficiencies in privacy theory can be traced to the methodologies that legal scholars of privacy commonly employ and the assumptions on which those methodologies are based. Like legal schol-

arship about copyright, legal scholarship about privacy is infused with the commitments of liberal political theory. As we saw in Chapter 3, those commitments do not function well at the self/culture intersection. Privacy concerns the boundary conditions between self and society, and the ways that those conditions mediate processes of self-formation. In U.S. legal scholarship about privacy, resistance to examining the complex relationship between self and society works systematically to undermine efforts at reconceptualizing privacy and to steer privacy theorists away from literatures that might help in that task.

Some privacy scholars argue that privacy is itself an artifact of liberal political theory. According to Peter Galison and Martha Minow, rights of privacy are inseparably tied to the liberal conception of the autonomous, prepolitical self. They argue that privacy as we know it (in advanced Western societies) ultimately will not withstand the dissolution of the liberal self diagnosed by contemporary social theory.[2] Privacy and liberal political theory are closely intertwined, but the problem of privacy is more complicated than that argument suggests. The understanding of privacy as tied to autonomy represents only one possible conception of privacy's relation to selfhood. More fundamentally although privacy is often linked to the liberal values of dignity and autonomy within our political discourse, it also conflicts with other liberal values. In the networked information society, protection for privacy compromises the liberal commitments to free flows of information, to the presumed equivalence between information and truth, and to the essential immateriality of personality. The conceptual gaps within privacy theory therefore reflect not only tensions between liberalism and critical theory, but also tensions internal to liberalism. As we will see, the gaps within privacy theory have very real consequences for the content of privacy law and policy.

The Subject of Privacy: The Autonomy Paradox

The first defect in privacy theory is the most fundamental, and concerns the relation between privacy and selfhood. Privacy rights attach to individuals, but how and why? Exactly who is the self that privacy is supposed to benefit? Within U.S. privacy theory, answers to those questions often invoke concepts of autonomy. But autonomy-based formulations of privacy interests raise more questions than they answer. Different strands of privacy doctrine suggest very different accounts of the way that privacy and autonomy are related, and those accounts are inconsistent both internally and with one another. The commitment to autonomy becomes even odder when it is situated in historical context. For nearly a century, the notion of the self-sufficient, autonomous individual has been under attack. Within social theory on both sides of the Atlantic, the autonomous self has given way to the socially constructed subject. Unlike their European and Canadian counterparts, however, most U.S. privacy theorists have resisted or avoided engaging with the insights and methods of contemporary social theory, and have interpreted those insights as undermining not only the idea of separation between self and society, but also the very idea of a self that might have privacy claims to assert.

It is instructive to begin our exploration of the "autonomy paradox" in privacy theory by considering accounts of the individual privacy claimant that emerge from privacy jurisprudence. As Neil Richards has demonstrated, strands

of U.S. constitutional jurisprudence establish robust privacy protection for thought, belief, and association; the asserted purpose of this protection is to nurture unconventional or dissenting thought that otherwise might be stifled by social disapproval.[3] Constitutional privacy jurisprudence also protects certain decisions that are viewed as intimately bound up with the definition of self, and again it does so to shield individuals making such decisions from the chill of majoritarian displeasure.[4] By way of parallel to the nomenclature developed in Chapter 3, I will call the presumed beneficiary of these doctrines the "romantic dissenter." The romantic dissenter is not, on the whole, a fragile figure; among other things, when she chooses to participate in the rough-and-tumble of the marketplace of ideas she will not be able to demand protection against those who disagree with her or against ad feminam attacks on her character. But her claim to privacy protection for her beliefs, associations, and intimate decisions is widely acknowledged. And if she chooses to speak anonymously, she often can invoke constitutional protection for that decision as well.[5]

The romantic dissenter also animates the strand of constitutional privacy doctrine that establishes privacy protection for homes and personal papers. Here too privacy functions as a safeguard against majoritarian tyranny. The home is conceptualized as a retreat from public life, affording shelter from public scrutiny of one's activities; in this respect, it complements the doctrines that protect intellectual privacy.[6] In addition, privacy protection for the home shelters activities that simply have no place in the public sphere.

The emerging U.S. legal framework for information privacy, which revolves primarily around the design of procedures for opting into or out of data collection, seems to contemplate a very different beneficiary of privacy protection.[7] This individual is concerned above all with maximizing his surplus in the marketplace. He may have preferences for privacy, but he regards those preferences and any formal entitlements to privacy as tradeable for other benefits that he might value more highly. I will call this privacy claimant the "rational chooser"; as with the economic user of copyrighted works, the rational chooser's implicit theoretical allegiance is to economic models of behavior and decision making.

As in the case of copyright, the first thing to notice about these characters is that they seem to exist only within their home domains. One can easily imagine the rational chooser consenting to have his communications or reading decisions monitored and to have trouble comprehending the chill that supposedly would result from allowing information about intimate decisions to be disclosed. Yet that view of appropriate privacy rules for belief, association, and the like is decidedly a minority one. Expressive and associational privacy, and to a lesser extent residential privacy, are the domains of the romantic dissenter. The romantic dissenter, meanwhile, might complain that the collection, use, and sale of information about her grocery purchases or her rental history chill her opportunities for self-development. Should she do so, she would have trouble finding a sympathetic audience. Within the structure of U.S. privacy law, commercial transactions are the domain of the rational chooser. The banal, de minimis nature of most such transactions has repeatedly frustrated efforts to reframe information privacy problems as implicating profound self-development concerns. Within common-law privacy doctrine, some uses of information do trigger higher levels of legal protection, but they involve falsity

or particularly intimate facts linked to the romantic dissenter's traditional concerns.

One explanation for the inconsistency might simply be that people have different expectations in different domains of activity and that those domains therefore demand different degrees of legal solicitude. If so, then arguably there is nothing inconsistent about protecting communications and associations to a greater extent than commercial transactions. Yet underlying the different sorts of rules for different kinds of privacy are some very different assumptions about the sorts of autonomy that individual privacy claimants exercise. Both the romantic dissenter and the rational chooser exercise autonomy, but the autonomy exercised by each is different. The rational chooser is a definitionally autonomous being who experiences unbroken continuity between preference and action; his choices are relatively impervious to outside influence, and so he neither wants nor needs privacy protection for them. The romantic dissenter requires privacy protection for her autonomy to flourish; as a practical matter, then, she exercises autonomy only to the degree that her environment enables it. If the rational chooser and the romantic dissenter were actually two different people, this might not be especially troubling. Since they are supposed to be the same person, the divergent conceptions of autonomy are worrisome.

The two different visions of the autonomy exercised by privacy claimants map to two different schools of thought about the nature of autonomy more generally. Within the framework of liberal political theory, the rational chooser corresponds to the conventional understanding of negative liberty as the absence of overt constraint. At any point in time, the autonomous self is definitionally capable of both choice and consent, and so we can say that autonomy subsists both in those choices and in the overall pattern that they establish. For other privacy theorists, however, this understanding of autonomy sets up an "autonomy trap."[8] These theorists argue that sometimes moment-to-moment choices need to be constrained so that people can become free to make better long-term choices than they otherwise might make. This position on autonomy corresponds to the conventional understanding of positive liberty as a freedom to choose wisely that cannot exist without some sort of environmental enablement. The romantic dissenter corresponds to this latter position; she requires rules that guarantee privacy of thought, belief, and association in order to develop her capacities to the fullest.[9]

The problem with the negative liberty framework is that when it is taken as a description of human capability, it is self-evidently false. Autonomous adults do not spring full-blown from the womb. Children and young adults must grow into their autonomy, and this complication introduces the problem of dynamic self-formation that the negative-liberty framework seeks to avoid. To know when an individual has attained the capacity for autonomous choice, we need to decide how much nurture is enough.

Within a positive-liberty framework, though, the search for the dividing line between "autonomy" and external influence presents a problem of infinite regress. Some privacy scholars, myself included, have attempted to finesse this problem by characterizing information-collection practices and privacy rules as intimately involved in the ongoing constitution of selfhood. Even as they highlight the dynamic nature of self-formation, however, these "constitutive privacy" scholars continue to insist on the existence of an autonomous core—an

essential self identifiable after the residue of influence has been subtracted.[10] The problem, however, is not simply that autonomy is constituted over time and by circumstances; it is that including autonomy in the definition of the ultimate good to be achieved invokes a set of presumptions about the separateness of self and society that begs the very question we are trying to answer.

The debate about underlying conceptions of autonomy in privacy law is a theoretical one, but its consequences are not. First, the divide between the different domains of privacy, and between the corresponding conceptions of autonomy, doesn't tell us what to do when those domains collide. These days, such collisions are more the rule than the exception. Is use of a computer system in the privacy of one's home to be governed by the rules that establish stringent privacy protection for activities at home or by the rather less stringent rules that govern privacy in commercial transactions with the providers of licensed software and communication networks? If the former, does taking one's laptop (or smart phone or personal digital assistant) outside one's home change the rules that apply? What privacy rules should apply to records showing purchases of intellectual goods? The romantic dissenter and the rational chooser can't answer these questions; we have no rules of encounter that might tell us how to reconcile their incompatible demands.

The figures of the romantic dissenter and the rational chooser, and the underlying conceptions of autonomy that they represent, also don't map to an assortment of other problems that are experienced by ordinary people as implicating privacy concerns. To begin with the most banal, they don't explain the desire for privacy for ordinary bodily functions. Activities such as excretion and sex are neither secret (everyone does them) nor romantic in their anatomical essentials, yet the view of them as private is strongly held. The romantic dissenter and the rational chooser also don't help us understand why most people assume that sharing personal details with one's airplane seatmate or one's circle of friends does not automatically equal sharing them with one's employer. Nor do they tell us why many people tend to feel that being subject to regularized surveillance in a public place is qualitatively different from simply being visible to others present there. In other words, they don't explain why most people understand privacy as a quality subject to an enormous amount of contextual variation.[11] Not coincidentally, privacy theory lacks good frameworks for understanding why these problems, none of which appears to implicate autonomy in any obvious way, nonetheless implicate (and often violate) the affected individuals' sense of self.

Ultimately, the autonomy paradox illustrates the ways in which the commitments of liberal political theory have constrained scholarly approaches to the self-society relation. Interrogating the conceptions of autonomy that exist in privacy theory exposes a deep conceptual poverty about what selves are made of. Straining to identify the point at which autonomy ends and influence begins does not take us very far toward answering that question. Within contemporary social theory, the separation between self and society that lies at the root of the autonomy paradox does not exist. From that perspective, a robust theory of privacy requires an understanding of the processes by which selfhood comes into being and is negotiated through contexts and over time. It is not obvious why that understanding should be attainable only by interrogating the

conditions of true independence. And yet privacy theory remains preoccupied with the latter inquiry.

In general, U.S. privacy scholars are deeply resistant, even hostile, to the idea of the socially constructed self. The aversion is so strong that many privacy theorists are unwilling to entertain even the more modest argument for "constitutive privacy"—which, as we have seen, manages at most a partial engagement with the problem of evolving subjectivity. Those scholars read the constitutive-privacy argument as completely inconsistent with liberty of choice and of belief. As Jeffrey Rosen puts it, "I'm free to think whatever I like even if the state or the phone company knows what I read."[12] That argument, which elides the distinction between social shaping and choice, is a product of the liberal conception of autonomy, pure and simple; social shaping negates choice only if choice is understood as requiring a perfect absence of influence.

That understanding of theories of social shaping is far too crude; social shaping need not entail the negation of self. One can choose to understand the autonomous liberal self and the dominated postmodernist subject as irreconcilable opposites, or one can understand them as two (equally implausible) endpoints on a continuum along which social shaping and individual liberty combine in varying proportions. By taking the latter perspective, moreover, it is possible to meld contemporary critiques of the origins and evolution of subjectivity with the more traditionally liberal concerns that have preoccupied American privacy theorists. Postmodernist social theory seeks to cultivate a critical stance toward claims to knowledge and self-knowledge. In a society committed at least to the desirability of the liberal ideal of self-determination, that perspective should be an appealing one. A theory of privacy for the information age should engage it and should explain what function privacy performs in a world where social shaping is everywhere and liberty is always a matter of degree.

The Social Value (or Cost?) of Privacy

Perhaps motivated by the autonomy paradox, some privacy theorists seek to formulate the value of privacy in purely social terms. That approach, however, leads rapidly to the second defect in privacy theory, which concerns the way in which accounts of the collective interest in privacy traditionally have been formulated. Arguments from collective interests typically do not engage directly with the asserted social justifications for seeking more information and so for denying privacy in specific cases. Instead, they advocate privacy by describing some other, incommensurable good that privacy advances. Arguing about whether a general preference for privacy should overcome instances of specific societal need passes over a critical moment in which the specific social need is effectively conceded and linked to a powerful general imperative that relates to the value of information and information processing: more information is better. Failure to challenge the information-processing imperative leaves privacy theory in an epistemological double bind. When it accedes to unrestricted flows of personal information, privacy theory betrays its own deepest commitments. When it proposes to restrict flows of information, privacy theory exposes itself to charges of Luddism and censorship. Failure to confront the assumptions on which those charges are founded amounts to an effective con-

cession that privacy is at odds not only with markets but also and more fundamentally with innovation and truth.

Many privacy theorists have approached the problem of the collective interest in privacy by defining it away. Some argue that the collective interest in privacy is a mirror of the individual interest, whatever that may be. On this interpretation, society's interest in privacy is reduced to ensuring that the individual's interest is fulfilled.[13] One obvious difficulty with this approach is that it succeeds only to the extent that we understand the nature of the individual interest. But presuming a perfect identity of social and individual interests also begs a question that deserves to be considered more carefully. It makes sense to think that society should want to promote individual flourishing, but a societal definition of human flourishing might include interpersonal goods and might value those goods differently than the affected individuals would. Other scholars position collective interests as inevitably opposed to individual ones. This oppositional understanding of privacy emerges most powerfully in communitarian political theory, which holds that the welfare of the community must take precedence over the welfare of the individual. A similar position is implicit in the work of other scholars who argue that security should be privileged over privacy in most cases.[14] Yet the oppositional understanding of privacy does not consider that society may have something to gain as well as something to lose by protecting privacy.

Within the last two decades, a number of scholars have made a more sustained effort to define privacy-related goods that are truly collective in nature. Although there are a number of differences in background and approach among these scholars, they are united in insisting that a just society is more than simply the aggregate of its individual members and that collective goods are more than simply the aggregate of individual goods. According to Robert Post and Ferdinand Schoeman, privacy promotes the formation and maintenance of civil society. Priscilla Regan, Radhika Rao, and Colin Bennett and Charles Raab argue that privacy protection promotes equality. Daniel Solove takes a different, avowedly pragmatist tack, arguing that privacy serves multiple goods, both individual and collective, that are intimately bound up with everyday experience.[15]

None of these theories about privacy's collective value, however, tells us what to do differently when it is time to balance privacy interests against other interests. Here Bennett and Raab look to process. Political scientists by training, they focus on the design of privacy institutions and on getting privacy and privacy advocates a seat at the bargaining table. But getting privacy onto the table brings us no closer to understanding how to balance the collective and individual interests in privacy against privacy's asserted costs. Instead, generalized concerns for privacy tend to give way to countervailing interests that are more crisply articulated.[16] Privacy theorists sometimes explain this outcome by using a version of the availability heuristic: it can be difficult to see how relaxing privacy standards in a particular case would jeopardize the value placed on civility or equality more generally. Overcoming this problem, they argue, requires even stronger, more compelling normative arguments about the social values that privacy serves.

While privacy theorists are right about the central role of normative judgment in privacy policy making (a question that I take up in more detail be-

low), they are wrong about where that normative judgment needs to kick in, and also wrong to blame the availability heuristic for breakdowns in the policy process. On the whole, privacy scholars do not interrogate the information-processing imperative on which the case against privacy rests. They do worry about error costs in privacy decision making; to oversimplify only slightly, privacy skeptics worry about false negatives in the realm of security (for example, overlooked terrorists) and false positives in the realm of commerce (for example, bad hiring decisions), while for privacy advocates, the problems are reversed (for example, innocent citizens unjustly detained and trustworthy job candidates mistakenly rejected). But debate about the magnitude and direction of the error rate elides important threshold questions about the validity of the challenged practices as information-processing practices.

On its face, this reluctance to dig more deeply is very odd. In other legal contexts, it is well recognized that information-processing practices reflect, and often create, social value judgments. In particular, historians and theorists of discrimination have drawn attention to the social construction of purportedly objective statistical "truths" about race, religion, and gender. As Frederick Schauer demonstrates at length, opposition to entrenched societal discrimination is hard to reconcile with commitment to the truth-value of information; the line between useful heuristics and invidious stereotypes is vanishingly thin. Effective antidiscrimination policy therefore requires the exercise of moral judgment about the value of information.[17]

Privacy scholars have strenuously resisted generalizing these conclusions from antidiscrimination theory to information processing more generally. More often, a sort of reverse generalization occurs: privacy theorists tend to think that the solution is better (information-based) metrics for separating the invidious frameworks from the truthful ones. Thus, for example, Lior Strahilevitz contrasts valuable "information" with wasteful "signals," and argues that privacy policy should encourage use of the former rather than the latter.[18] That seems reasonable enough, but it assumes an ontological distinction between the two categories that does not exist. Jeffrey Rosen worries about the risk of "being misdefined and judged out of context in a world of short attention spans."[19] That statement expresses a commendable doubt about the human capacity to judge, but it sidesteps the question of information value. The worry about any particular piece of information is that we will not take the time and effort to weigh it properly, not that the information is somehow wrong "in itself." Still other privacy scholars argue that flows of personal information are best understood as speech protected by constitutional guarantees of expressive liberty. On that view, laws protecting privacy can prohibit trade only in information that is provably false.

When privacy scholars' reluctance to confront the information-processing imperative is situated within the tradition of liberal political theory, it becomes much less mysterious. The information-processing imperative comes to us directly from the Enlightenment; it is grounded in a view of information gathering as knowledge discovery along a single, inevitable trajectory of forward progress. Within that philosophical framework, the interest in getting and using more complete information is presumptively rational and entitled to deference. The truth-value of "more information" is assumed and elevated to a level beyond ideology; as a result, the other work that information processing

does goes unaddressed and usually unacknowledged. The free-speech argument against privacy invokes a related ideology about knowledge discovery in the "marketplace of ideas": even if some speech is wrong or irrelevant, truth will emerge victorious so long as the flow of information is allowed to proceed unimpeded.

Faith in the ultimate truth-value of information, however, leads in both theory and policy to a series of rapidly cascading failures to hold back an inevitable tide. If information is always true but only sometimes relevant, where should the law draw lines? Unsurprisingly, attempts to isolate neutral rules of decision have been singularly unsuccessful. Within a liberal market economy, it is an article of faith that both firms and individuals should be able to seek and use information that (they believe) will make them economically better off. Businesses, in particular, want consumer personal information both to minimize foreseeable losses and to structure expected gains. Information reduces the uncertainty that accompanies any new venture because it affords access to a set of conventions for evaluating risk and profit potential. In disciplines ranging from marketing to actuarial science to finance, information processing transforms guesses into their more respectable cousins, estimates and projections, which in turn support the development of new products and industries.[20] Information also is bound up with discussions of risk and security in the public policy arena. In those discussions, every piece of information is presumptively relevant to the task of identifying and countering national security threats.

Faith in the truth-value of information reaches its zenith in processes of risk management, but the information-processing imperative also pervades other areas of activity. In legal disputes, in which uncertainty complicates questions of responsibility and remedy, every piece of information is presumptively relevant to the calculus of liability or guilt. For the modern welfare state, complete information is important to the determination of benefits. In many of these latter contexts, beliefs about the relationships between information and truth are also rooted in another foundational principle of the liberal tradition: the notion that respect for individual autonomy requires individualized treatment. Yet that argument too militates in favor of more information, not less. Whether the starting point is truth or dignity, the rationale for considering particular items of personal information rapidly becomes an argument in favor of collecting and using every piece of information that can be obtained.

Once again, many intellectual resources that might prove helpful to the project of interrogating the information-processing imperative have been placed off limits by liberal legal theorists' profound distrust of contemporary social theory. In particular, legal theorists' perception of postmodernism's deep commitment to moral and epistemological relativism tends to foreclose the possibility that its insights about the social construction of knowledge might prove useful. If, for example, postmodernism cannot claim to help privacy theory make moral judgments about the appropriate content of antidiscrimination law, or offer concrete policy recommendations that might provide comforting certainty to businesses and governments, then what good is it?

Again, though, that understanding of postmodernism's lessons is too simple. Systems of knowledge can be both contingent and deeply rooted, arbitrary in an absolute sense and yet deeply intertwined with norms and ways of living. What literatures about the construction of knowledge afford, and liberal

political theory typically does not, is access to the genealogy of a society's moral and intellectual commitments—to the ontological relationship between knowledge and moral, legal, and economic power. This in turn affords a vantage point of partial separation, a position of skepticism from which to interrogate existing presumptions and practices.

Specifically, literatures outside the liberal canon bear on three large and interlocking sets of problems that privacy theory needs to confront. First, they expose the ways in which practices and policies about information processing construct knowledge, including knowledge about the subjects of the emerging information society. Second, they provide resources with which to engage social and institutional preoccupations with risk and security. Third, they enable investigation and description of the ways in which categorization comes to support elaborate social, technical, and institutional infrastructures. In each of these areas, a more skeptical stance toward the information-processing imperative would enable privacy scholars and policy makers to interrogate claims about necessity and efficacy more effectively. In addition, it would enable privacy theorists to offer a more coherent account of the collective interest in limiting information processing and of the ways in which that interest intersects with the problem of self-formation.

The Nature of Privacy Harms

The final conceptual defect in scholarly accounts of privacy concerns the ways that the metaphoric structuring of privacy discourse affects our understanding of privacy and privacy harms. Unlike copyright scholars, privacy scholars are acutely sensitive to the recurrence of spatial metaphors in privacy discourse. Most have reacted negatively to the spatial metaphorization of privacy expectations and interests. For the most part, however, privacy scholars have not carefully investigated the roles that spatial metaphors play in privacy discourse. At the same time, they do not seem to notice the extent to which legal conceptions of privacy interests and harms are structured predominantly by visual metaphors.

Since the U.S. 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, and a homeowner is not necessarily entitled to protection against direct visual observation by airplane overflight, nor to privacy in items left out for garbage collection.[21] Employees sometimes can assert privacy interests against undisclosed workplace surveillance.[22]

For my purposes here, 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* (2001), which involved the use of heat-sensing technologies to detect indoor marijuana cultivation, was styled as a ringing reaffirmation of the traditional privacy interest in the home, but in fact upholds that interest only against information-gathering technologies "not in general public use."[23] Similarly, although legal scholars disagree about the precise nature of the privacy interest, they seem to agree that cognizable injury would require the involvement of a human observer who perceives or receives information.[24] 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. Instead, both courts and scholars are enormously critical of spatial metaphors in privacy discourse. The Supreme Court has expressed reluctance to extend spatial conceptions of privacy outside the physical space of the home. In *United States v. Orito* (1973), the majority characterized the dissenters' formulation of the privacy interest as a "sphere" that accompanies each individual as lacking any limiting principle. In fact, that conclusion does not necessarily follow—or rather, it follows only if the privacy interest, once recognized, must be absolute, and that is what the Court read the "sphere" metaphor to imply.[25]

Like the *Orito* Court, many privacy theorists are deeply uncomfortable with spatial metaphors in privacy discourse. These scholars tend to offer four principal reasons for their resistance to spatialization. First, some scholars object that the spatialization of privacy interests reinforces doctrinal links between privacy and property. This undermines claims to privacy in public spaces and also undermines claims to privacy in spaces and across communication networks owned by third parties. *Kyllo* has been roundly criticized precisely for seeming to make the physical space of the private home a preeminent consideration. Second and relatedly, some scholars assert that links between privacy and property reinforce and perpetuate social and economic relations of inequality. They note that historically, privacy linked to property has insulated domestic abuse and corporate discrimination from public scrutiny. Third, some scholars assert that spatial metaphors in privacy discourse are too imprecise to be useful. Thus, for example, Lloyd Weinreb observes that spatial metaphors for privacy "do[] not specify at all the shape or dimensions of the space or what it contains."[26] Finally, many privacy scholars argue that spatial metaphors are unhelpful in the networked information society because the greatest threats to privacy arise from the pervasive collection and sharing of information.

And yet spatial metaphors continue to recur in privacy discourse. Even in contexts that are not thought to involve spatial privacy at all, judges routinely and unselfconsciously refer to "spheres" and "zones" to describe privacy interests. Spatial metaphors for privacy appear particularly often in concurring and dissenting opinions in which judges are attempting to explain their understanding of the privacy to which individuals ought to be entitled and that the law

should attempt to guarantee.[27] Despite the insistent drumbeat of scholarly criticism, spatial metaphors also populate the scholarly literature on privacy. Articles on information privacy contain numerous references to "zones" and "spheres" of privacy, and these terms do not refer only to defined physical spaces. Instead, they position privacy more generally as a sort of metaphorical shelter for the self.[28]

Even as they criticize spatial metaphorization, privacy theorists often seem oblivious to the predominance of visual metaphors in privacy discourse. An implicit linkage between privacy and visibility is deeply embedded in privacy doctrine. The body of constitutional privacy doctrine that defines unlawful searches regulates tools that enable law enforcement to "see" activities as they are taking place inside the home more strictly than tools for discovering information about those activities after they have occurred. *Kyllo* was deemed worthy of Supreme Court consideration precisely because it seemed to lie on the boundary between those categories. 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. The informational torts, unauthorized publication and false light, are far more stringently limited (to "embarrassing" private facts and to falsity).[29] Efforts to develop a more robust informational privacy tort have confronted great skepticism, for reasons that seem closely linked to conventions about visibility. Litigants 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.[30] Information-privacy skeptics, meanwhile, have argued that privacy interests cannot attach to information voluntarily made "visible" as part of an otherwise consensual transaction.[31]

Over the last decade, the principal contribution of what has been dubbed the "information privacy law project" has been to refocus both scholarly and popular attention on the ways in which techniques of information collection operate to render individuals and their behaviors accessible in the networked information age. Many contemporary legal and philosophical theories of privacy are organized explicitly around problems of information privacy and "privacy in public." These theories might be read to 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 one another in important respects, an implicit premise of all of them is that databases and personal profiles can communicate as much as or more than images. 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 identification of visual-surveillance subjects and subsequent searches of stored visual and data-based surveillance records.[32]

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. Solove, for example, argues that for the most part, informational accessibility does not result from a conscious decision

to target particular individuals; instead, accessibility is embedded in the design of social and technical institutions. Even so, he uses the term "digital dossier" to describe the threat that institutions insufficiently protective of privacy create. The digital dossier is a form of "unauthorized biography"; a way of representing the individual to the gaze of the world.[33]

Even as information-privacy theorists have sought to shift the focus of the discussion about privacy interests, moreover, 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 consisted of cells concentrically arranged around a central guard tower, from which the prison authority might see but not be seen. Architecturally and also etymologically, Bentham's conception suggests that direct visual observation by a centralized authority is the best exemplar of surveillance for social control. Important work in information privacy often invokes the Panopticon and other visual metaphors to drive home arguments about information-based risk.[34] Although Solove critiques Big Brother, his preferred metaphor of a hidden, dehumanized bureaucracy also is heavily reliant on visuality—the problem is precisely that privacy invasion lacks a "face" of its own.[35]

Why do privacy theorists find spatial metaphors for privacy so troubling and visual metaphors so compelling? Situating privacy theory within liberalism's legacy of mind-body dualism goes a long way toward explaining the mismatch between the official privacy discourse of visibility and the unofficial privacy discourse of spaces, zones, and spheres. The understanding of privacy and privacy invasion as transcending space and physicality resonates powerfully with the liberal understanding of the self as abstract and disembodied. Bodies exist in spaces that are concrete and particular; vision is general and abstract, linked metaphorically with the transcendent power of reason.

From this perspective, it is not particularly surprising that the paradigm cases of privacy invasion should be conceptualized in terms of sight. 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." Cartesian philosophy of mind posits that objects and ideas exist "in the field of mental vision," where truth is "illuminated" by the "'light of Reason.'"[36] In the language of 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 and for that process to operate relatively unselfconsciously.

Yet that 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, if privacy invasion consists in being visible to Big Brother, then identifying privacy problems

becomes analytically more difficult when there is no single Big Brother at which to point.[37] And if visibility is linked to truth, it makes sense that privacy claimants often lose in the courts and before Congress. But knowledge, power, and sight are not the same. If "privacy" really is meant to denote an effective barrier to knowledge or to the exercise of power by others, equating privacy invasion with visibility assumes what ought to be carefully considered.

Privacy theory lacks a good account of either the official privacy discourse of visibility or the unofficial privacy discourse of spaces, zones, and spheres, and it needs both if it is to accomplish the task it has set for itself. The way that we talk about privacy shapes our understanding of what it is—and what it is not. Without careful consideration of the work that visual and spatial metaphors do in privacy discourse, it is impossible to have a rigorous discussion about why privacy matters and what kind(s) of privacy the law ought to protect. More concretely, a theory of privacy for the networked information society must address privacy problems in a way that corresponds to the experiences and expectations of real people. Perhaps we should understand the persistent recurrence of privacy concerns around bodies and spaces as telling us something important about the nature of privacy and privacy invasion as experienced. As we saw in Chapter 2, rich and vibrant literatures across a wide range of disciplines suggest that the relation between self and society is not, and never has been, a purely informational one, but rather is materially and spatially mediated. Privacy law and theory need to recognize the importance of bodies and spaces before the account of privacy interests can be complete.

Challenges for Privacy Theory

Finding a viable way forward for privacy theory and policy will require an approach that is temperamentally postliberal and methodologically eclectic. Liberal ideals of selfhood may furnish important aspirational guideposts for that inquiry, but access to the full range of contemporary thinking on the social and cultural aspects of the human condition is essential. Conceptualizing the subject of privacy requires a theory of socially situated subjectivity—a theory of the subject that is less unitary than liberalism's account of the separate self, but more robust than a mere subject position. In addition, it requires a set of disciplinary resources that interrogate the value of information-processing practices and that situate ongoing processes of self-formation in the concrete cultural and material contexts inhabited by real, embodied people. Chapter 6 considers what such a theory of privacy might contain.

Notes

[1] For a useful overview of the survey evidence and of behavioral and cognitive factors affecting consumer behavior, see Nehf, "Shopping for Privacy Online," 6-32.

[2] Galison & Minow, "Our Privacy, Ourselves."

[3] Richards, "Intellectual Privacy."

[4] DeCew, *In Pursuit of Privacy*, 77-78. See, for example, Roe v. Wade, 410 U.S. 113 (1973); Eisenstadt v. Baird, 405 U.S. 438 (1972); Griswold v. Connecticut, 381 U.S. 479 (1965).

[5] See, for example, Watchtower v. Village of Stratton, 535 U.S. 150 (2002); McIntyre v. Ohio Elections Comm'n, 514 U.S. 334 (1995).

[6] For good discussions of the history and purposes of constitutional protection against unreasonable searches and seizures, see Harris v. United States, 331 U.S. 145, 155-74 (1947) (Frankfurter, J., dissenting); Boyd v. United States, 116 U.S. 616, 625-32 (1886).

[7] For an example, see the Gramm-Leach-Bliley Act, Pub. L. No. 106–102, 113 Stat. 1437 (codifed at 15 U.S.C. §6802(b)). Exceptions involve information-gathering activities that relate to intellectual privacy and therefore implicate the romantic dissenter. See, for example, the Video Privacy Protection Act, Pub. L. No. 100–618, 102 Stat. 3195 (codified at 18 U.S.C. §2710); Richards, "Intellectual Privacy," 387 (summarizing state laws mandating privacy protections for library records).

[8] See Schwartz, "Privacy and Democracy in Cyberspace," 1660-62.

[9] For classic expositions of the negative liberty thesis and the positive liberty thesis, see Berlin, *Two Concepts of Liberty*, and Raz, *The Morality of Freedom*.

[10] See Allen, "Coercing Privacy"; Cohen, "Examined Lives"; Schwartz, "Privacy and Democracy in Cyberspace."

[11] For a perceptive analysis of privacy and contextual variation, see Nissenbaum, *Privacy in Context*.

[12] Rosen, *The Unwanted Gaze*, 166.

[13] See, for example, Rosen, *The Unwanted Gaze*.

[14] For the communitarian argument, see Etzioni, *The Limits of Privacy*. For the argument from security, see Posner, "Privacy, Surveillance, and Law," 245.

[15] See Bennett & Raab, *The Governance of Privacy*; Post, "The Social Foundations of Privacy"; Rao, "A Veil of Genetic Ignorance?"; Regan, *Legislating Privacy*; Schoeman, *Privacy and Social Freedom*; Solove, *Understanding Privacy*.

[16] For a perceptive discussion of the process by which privacy concerns give way to countervailing interests, see Regan, *Legislating Privacy*.

[17] Schauer, *Profiles, Probabilities, and Stereotypes*.

[18] Strahilevitz, "Privacy versus Antidiscrimination," 376-81.

[19] See Rosen, *The Unwanted Gaze*, 8, 55-56, 198-06. In a similar vein, some economically inclined privacy scholars argue that the phenomenon of bounded rationality may mean that privacy has a valuable role to play in saving us from ourselves. See Strandburg, "Privacy, Rationality, and Temptation."

[20] On the constitutive importance of risk and risk management in contemporary economic and social organization, see Beck, *Risk Society*.

[21] On privacy protection for residential tenants, see Hamberger v. Eastman, 206 A.2d 239, 242 (N.H. 1964). On airplane overflight, see Florida v. Riley, 488 U.S. 445, 451 (1989); California v. Ciraolo, 476 U.S. 207, 214-15 (1986). On privacy interests in garbage, see California v. Greenwood, 486 U.S. 35, 40 (1988).

[22] See O'Connor v. Ortega, 480 U.S. 709, 713-14 (1987); Mancusi v. DeForte, 392 U.S. 364, 369 (1968).

[23] Kyllo v. United States, 533 U.S. 27, 34 (2001).

[24] See, for example, Lisa Austin, "Privacy and the Question of Technology," 126; Gavison, "Privacy and the Limits of Law," 432.

[25] United States v. Orito, 413 U.S. 139, 142-43 (1973).

[26] Weinreb, "The Right to Privacy," 26-27.

[27] In constitutional privacy case law, the "zone" metaphor originates in Griswold v. Connecticut, 381 U.S. 479, 484-85 (1965). For examples of subsequent federal cases invoking the "zone" and "sphere" metaphors, see Ohio v. Akron Center for Reproductive Health, 497 U.S. 502, 529-32 (1990) (Blackmun, J., dissenting); New Jersey v. T.L.O., 469 U.S. 325, 361 (Brennan, J., dissenting); Rakas v. Illinois, 439 U.S. 128, 159-60, 164 (1978) (White, J., dissenting); Zablocki v. Redhail, 434 U.S. 374, 397 (1978) (Powell, J., concurring); Dietemann v. Time, Inc., 449 F.2d 245, 248-49 (9th Cir. 1971). For examples of state privacy tort cases employing the "zone" and "sphere" metaphors, see Shulman v. Group W Productions, Inc., 955 P.2d 469, 498 (Cal. 1998); Stall v. Long, 570 So. 2d 257, 269 (Fla. 1990); Young v. Jackson, 572 So. 2d 378, 381 (Miss. 1990); Luedtke v. Nabors Alaska Drilling, Inc., 768 P.2d 1123, 1135-36 (Alaska 1989); Rhinehart v. Seattle Times Co., 654 P.2d 673, 679-82 (Wash. 1982); Multimedia WMAZ, Inc. v. Kubach, 443 S.E.2d 491, 499 (Ga. Ct. App. 1994); Urbaniak v. Newton, 277 Cal. Rptr. 354, 357-61 (Cal. Ct. App. 1991).

[28] See, for example, Schartum, "Designing and Formulating Data Protection Laws," 2 ("I understand 'privacy' to be a concept that first and foremost expresses the state in which a person is inaccessible to others, for instance within a private sphere"); Schwartz, "Preemption and Privacy," 907 ("Tort privacy . . . creates a legal process for negotiation of limits . . . on the individual's desire for zones of privacy without community scrutiny"); Strahilevitz, "Reputation Nation," 1736 ("True enough, the private sphere of the home will remain a respite . . . and there will be market demand for zones of privacy"); West, "The Story of Us," 594 ("[W]hile it is troubling to give Henry the ability to silence Emily, it is a matter of no small concern that Emily is in a position to destroy Henry's personal zone of privacy").

[29] For an overview of the common-law privacy torts, see Keeton, *Prosser and Keeton on the Law of Torts*, §117, 851-56.

[30] See, for example, Dwyer v. American Express Co, 652 N.E.2d 1351, 1355-56 (Ill. App. Ct. 1995); Castro v. NYT Television, 851 A.2d 88, 98 (N.J. Super. Ct. 2004).

[31] See, for example, Singleton, "Privacy versus the First Amendment," 121-33.

[32] For a good overview of this literature and for the "project" nomenclature, see Richards, "The Information Privacy Law Project." On the particular problem of privacy in public, see Nissenbaum, *Privacy in Context*, 113-26; Nissenbaum, "Protecting Privacy in an Information Age."

[33] Solove, *Digital Person*, 44-47.

[34] See, for example, Lyon, *The Electronic Eye*; Rosen, *Unwanted Gaze*; Reiman, "Driving to the Panopticon." For the classic analysis of the Panopticon, see Foucault, *Discipline and Punish*, 200-09.

[35] Solove, *Digital Person*, 36-41.

[36] Descartes, *Rules for the Direction of Mind*. On the iconography of the linkage between vision, knowledge, and power, see Schmidt-Burkhardt, "The All-Seer," 18-26.

[37] Solove, *Digital Person*, 33-35.