WHAT PRIVACY IS FOR

*Julie E. Cohen**

I. HOW PRIVACY GOT A BAD NAME FOR ITSELF

Privacy has an image problem. Over and over again, regardless of the forum in which it is debated, it is cast as old-fashioned at best and downright harmful at worst — antiprogressive, overly costly, and inimical to the welfare of the body politic.[1] Privacy advocates resist this framing but seem unable either to displace it or to articulate a comparably urgent description of privacy's importance. No single meme or formulation of privacy's purpose has emerged around which privacy advocacy might coalesce.[2] Pleas to "balance" the harms of privacy invasion against the asserted gains lack visceral force.

The consequences of privacy's bad reputation are predictable: when privacy and its purportedly outdated values must be balanced against the cutting-edge imperatives of national security, efficiency, and entrepreneurship, privacy comes up the loser.[3] The list of priva-

---

* Professor, Georgetown University Law Center. Thanks to Michael Birnhack, Deven Desai, Laura Donohue, Andrew Glickman, James Grimmelmann, Frank Pasquale, Daniel Solove, Valerie Steeves, participants in the *Harvard Law Review* Symposium on Privacy and Technology, and faculty workshop participants at Georgetown University Law Center for their helpful comments and provocations, and to Allegra Funsten and Kristina Goodwin for research assistance.

[1] *See, e.g.*, *Balancing Privacy and Innovation: Does the President's Proposal Tip the Scale?: Hearing Before the Subcomm. on Commerce, Mfg. & Trade of the H. Comm. on Energy & Commerce*, 112th Cong. 13 (2012) (statement of Rep. Marsha Blackburn, Member, H. Comm. on Energy & Commerce) (preliminary transcript); STEWART A. BAKER, SKATING ON STILTS: WHY WE AREN'T STOPPING TOMORROW'S TERRORISM 309–20 (2010) ("The right to privacy was born as a reactionary defense of the status quo, and so it remains." *Id.* at 312.); Heidi Reamer Anderson, *The Mythical Right to Obscurity: A Pragmatic Defense of No Privacy in Public*, 7 I/S: J.L. & POL'Y FOR INFO. SOC'Y 543, 549 (2012); Kent Walker, *Where Everybody Knows Your Name: A Pragmatic Look at the Costs of Privacy and the Benefits of Information Exchange*, 2000 STAN. TECH. L. REV. 1, 1; Fred H. Cate, *Invasions of Privacy? We'll All Pay Cost if We Cut Free Flow of Information*, BOS. GLOBE, Sept. 2, 2001, at D8; *FTC Cautioned Against Heavy Privacy Rules*, COMM. DAILY, Feb. 25, 2011, at 3; Jim Harper, *It's Modern Trade: Web Users Get as Much as They Give*, WALL ST. J., Aug. 7–8, 2010, at W1; Lee Gomes, *The Hidden Costs of Privacy*, FORBES (May 20, 2009, 6:00 PM), http://www.forbes.com/forbes/2009/0608/034-privacy-research-hidden-cost-of-privacy.html; Bobbie Johnson, *Privacy No Longer a Social Norm, Says Facebook Founder*, GUARDIAN (Jan. 10, 2010, 8:58 PM), http://www.guardian.co.uk/technology/2010/jan/11/facebook-privacy.

[2] On the framing dilemmas that surround privacy advocacy, see COLIN J. BENNETT, THE PRIVACY ADVOCATES 2–21 (2008).

[3] For a detailed exploration of this dynamic at work in legislative and policy debates about information privacy, communications privacy, and polygraph testing, see PRISCILLA M. REGAN, LEGISLATING PRIVACY: TECHNOLOGY, SOCIAL VALUES, AND PUBLIC POLICY (1995). For a description of the substantive incoherence of the balancing paradigm, see COLIN J. BENNETT &

cy's counterweights is long and growing. The recent additions of social media, mobile platforms, cloud computing, data mining, and predictive analytics now threaten to tip the scales entirely, placing privacy in permanent opposition to the progress of knowledge.

Yet the perception of privacy as antiquated and socially retrograde is wrong. It is the result of a conceptual inversion that relates to the way in which the purpose of privacy has been conceived. Like the broader tradition of liberal political theory within which it is situated, legal scholarship has conceptualized privacy as a form of protection for the liberal self. So characterized, privacy is reactive and ultimately inessential. Its absence may at times chill the exercise of constitutionally protected liberties, but because the liberal self inherently possesses the capacity for autonomous choice and self-determination, loss of privacy does not vitiate that capacity. As this Article explains, however, such thinking is mistaken.

In fact, the liberal self who is the subject of privacy theory and privacy policymaking does not exist. As Part II discusses, the self who is the real subject of privacy law and policy is socially constructed, emerging gradually from a preexisting cultural and relational substrate. For this self, privacy performs a function that has nothing to do with stasis. Privacy shelters dynamic, emergent subjectivity from the efforts of commercial and government actors to render individuals and communities fixed, transparent, and predictable. It protects the situated practices of boundary management through which the capacity for self-determination develops.

So described, privacy is anything but old-fashioned, and trading it away creates two kinds of large systemic risk, which Parts III and IV describe. Privacy incursions can be episodic or systematic, but systematic deprivations of privacy also facilitate episodic privacy incursions. In this Article, therefore, I focus on the interplay between privacy and systems of surveillance. Part III argues that freedom from surveillance, whether public or private, is foundational to the practice of informed and reflective citizenship. Privacy therefore is an indispensable structural feature of liberal democratic political systems. Freedom from surveillance also is foundational to the capacity for innovation; therefore, as Part IV explains, the perception of privacy as anti-innovation is a non sequitur. Innovation occurs in commercial and social contexts and is infused with particular commercial and social values. A commercial culture that sees privacy as threatening its own valued practices of knowledge production will register privacy regulation as a threat. But a society that values innovation ignores

---

CHARLES D. RAAB, THE GOVERNANCE OF PRIVACY: POLICY INSTRUMENTS IN PERSPECTIVE 8–14 (2006).

privacy at its peril, for privacy also shelters the processes of play and experimentation from which innovation emerges. In short, privacy incursions harm individuals, but not only individuals. Privacy incursions in the name of progress, innovation, and ordered liberty jeopardize the continuing vitality of the political and intellectual culture that we say we value.

A structural understanding of privacy's importance demands a structural approach to privacy regulation. Effective privacy protection requires comprehensive attention to the systemic attributes of both public and private surveillance practices, and to the ways in which public and private surveillance practices supplement and reinforce one another. Part V briefly outlines some strategies for achieving these goals. Effective privacy regulation must render both public and private systems of surveillance meaningfully transparent and accountable. It also must preserve breathing room for practices of boundary management by situated subjects. Dynamic, emergent subjectivity — the sort of subjectivity upon which liberal democracy and innovation both rely — thrives in the interstitial spaces within information-processing frameworks; privacy regulation must focus on maintaining those spaces.

II. PRIVACY AND FREEDOM, REIMAGINED: PRIVACY'S DYNAMISM

Privacy's bad reputation has deep roots in privacy theory. This Part traces those roots to the tradition of liberal individualism, which supplies both the conventional understanding of the self that privacy is thought to protect and the criteria that an intellectually defensible theory of the right to privacy must satisfy.[4] Neither set of commitments has served privacy theory well. The self who benefits from privacy is not the autonomous, precultural island that the liberal individualist model presumes. Nor can privacy be reduced to a fixed condition or attribute (such as seclusion or control) whose boundaries can be crisply delineated by the application of deductive logic. Privacy is shorthand for breathing room to engage in the processes of boundary management that enable and constitute self-development. So understood, privacy is fundamentally dynamic. In a world characterized by pervasive social shaping of subjectivity, privacy fosters (partial) self-determination. It enables individuals both to maintain relational ties and to develop critical perspectives on the world around them.

Scholarship about privacy within the U.S. legal academy is infused with the commitments of liberal political theory, first and foremost of

---

[4] For a more detailed analysis, see JULIE E. COHEN, CONFIGURING THE NETWORKED SELF: LAW, CODE, AND THE PLAY OF EVERYDAY PRACTICE 16–20, 107–26 (2012).

which is a conception of the self as inherently autonomous. In its ideal form, the liberal self possesses both abstract liberty rights and the capacity for rational deliberation and choice and is capable of exercising its capacities in ways uninfluenced by cultural context. Not all privacy scholars subscribe to this vision in its purest form; like liberal political theorists more generally, privacy scholars disagree about whether autonomy is most appropriately characterized as negative or positive liberty. Some endorse the negative liberty paradigm, arguing that privacy is best understood as an exercise of personal choice.[5] Others argue that privacy is a vital enabler of positive liberty and that individuals therefore need considerable privacy protection to attain the independence that the liberal model assumes.[6] All seem to agree, however, that the self possesses "an autonomous core — an essential self identifiable after the residue of influence has been subtracted."[7] The positive liberty paradigm, moreover, has made little headway within U.S. privacy policy, which is dominated instead by a commitment to notice and choice that derives from the negative liberty paradigm. For the autonomous self, privacy's function is principally defensive and ameliorative. Privacy preserves negative space around individuals who are already fully formed or mostly fully formed, affording shelter from the pressures of societal and technological change. That understanding of privacy links it inseparably to stasis.

As this brief summary of the debate about privacy and autonomy suggests, efforts to theorize privacy also have been hampered by the methodological commitments of liberal political theory, which prize most highly those definitions of rights that are susceptible to formal, quasi-scientific derivation from core principles. Most privacy theorists have tended to think that the key to defining privacy lies in locating privacy's essence in one or another overarching principle (such as liberty, inaccessibility, or control) and then offering finely parsed resolutions of the resulting conflicts between the principles and ordinary, everyday practices and expectations.[8] Definitions of privacy grounded in core principles, however, inevitably prove both over- and underinclusive when measured against the types of privacy expectations that

---

[5] *See* LARRY DOWNES, A RATIONAL RESPONSE TO THE PRIVACY "CRISIS," 26–31 (Cato Inst. Policy Analysis No. 716, 2013), *available at* http://www.cato.org/sites/cato.org/files/pubs/pdf/pa716.pdf; Judith Jarvis Thomson, *The Right to Privacy*, *in* PHILOSOPHICAL DIMENSIONS OF PRIVACY: AN ANTHOLOGY 272, 279–81 (Ferdinand David Schoeman ed., 1984).

[6] *See* Anita L. Allen, *Coercing Privacy*, 40 WM. & MARY L. REV. 723, 738–40 (1999); Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1656–58 (1999). I include in this category my own earlier work. *See* Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1424–25 (2000).

[7] *See* COHEN, *supra* note 4, at 113.

[8] A magisterial exploration of privacy's conflicts with principles of liberty is ANITA L. ALLEN, UNPOPULAR PRIVACY (2011).

real people have.[9] For example, such definitions can't explain the widespread belief that sharing personal details with one's friends or one's airplane seatmate does not automatically equal sharing them with one's employer. In the real world, privacy expectations and behaviors are unruly and heterogeneous, persistently defying efforts to reduce them to neat conceptual schema.

The irony in all this is that privacy theory's frustrations are largely self-inflicted. The idea of privacy as a defensive bulwark for the autonomous self is an artifact of a preexisting cultural construction; it does not reveal anything inevitable either about privacy or about selfhood. In fact, liberal privacy theory's descriptive premises about both the self and the nature of privacy are wrong. The self has no autonomous, precultural core, nor could it, because we are born and remain situated within social and cultural contexts. And privacy is not a fixed condition, nor could it be, because the individual's relationship to social and cultural contexts is dynamic. These realities do not weaken the case for privacy; they strengthen it. But the nature and importance of privacy can be understood only in relation to a very different vision of the self and of the self-society connection.

The way forward for privacy theory in the liberal tradition requires engaging with other scholarly traditions that acknowledge the emergent and relational character of subjectivity. One place to begin is with literatures in the fields of cognitive science, sociology, and social psychology, which establish empirical foundations for an understanding of subjectivity as socially constructed. These literatures explore the processes of gradual self-differentiation that individuals undergo beginning in early childhood, and probe the ways in which cognition is informed by linguistic and cultural conventions.[10] They also illuminate the various physical, spatial, and informational strategies that people deploy to manage their personal boundaries dynamically over time.[11]

Empirical accounts of emergent subjectivity converge with theoretical accounts of self-formation grounded in other major philosophical traditions, including postmodernism, phenomenology, and pragmatism. Postmodernist accounts of self-formation tend to emphasize the power

---

[9] For a more detailed discussion of the under- and overinclusiveness of reductive conceptions of privacy, see DANIEL J. SOLOVE, UNDERSTANDING PRIVACY 14–38 (2008).

[10] *See generally, e.g.*, DOROTHY HOLLAND, WILLIAM LACHICOTTE JR., DEBRA SKINNER & CAROLE CAIN, IDENTITY AND AGENCY IN CULTURAL WORLDS (1998); GEORGE LAKOFF & MARK JOHNSON, METAPHORS WE LIVE BY (1980); EVIATAR ZERUBAVEL, SOCIAL MINDSCAPES: AN INVITATION TO COGNITIVE SOCIOLOGY (1997); Paul DiMaggio, *Culture and Cognition*, 23 ANN. REV. SOC. 263 (1997).

[11] *See generally, e.g.*, IRWIN ALTMAN, THE ENVIRONMENT AND SOCIAL BEHAVIOR: PRIVACY, PERSONAL SPACE, TERRITORY, CROWDING (1975); CHRISTENA NIPPERT-ENG, ISLANDS OF PRIVACY (2010).

relationships at work in processes of social construction, while pragmatist accounts are more optimistic about the scope of individual agency.[12] Both traditions, however, are concerned with evolving subjectivity and with the formative power of culture and experience. Contemporary phenomenological theory explores the ways in which the experience of subjectivity is rooted in and mediated by the body and the material world.[13] Some of the most fruitful work in privacy theory today is being done at the intersection of these approaches.[14]

The goal of this synthesis is not, as some might have it, an illiberal model of selfhood.[15] That mode of reasoning — "if not liberal, then illiberal" — is not unusual, but it is unproductive. It is a product of the reflexive distancing too often practiced by members of different academic tribes rather than of any ineluctable reality. Selfhood and social shaping are not mutually exclusive. Subjectivity, and hence selfhood, exists in the space between the experience of autonomous selfhood and the reality of social shaping. It is real in the only way that counts: we experience ourselves as having identities that are more or less fixed. But it is also malleable and emergent and embodied, and if we are honest, that too accords with experience. Although reluctant to grapple directly with the social construction of subjectivity, important contemporary privacy theorists working within the liberal tradition emphasize the importance of contexts, spaces, bodies, and relationships for a theory of privacy.[16] This suggests tacit acknowledgment of the need for a postliberal theory of selfhood — one capacious enough to accommodate the full spectrum of relational, emergent subjectivity.

---

[12] Important examples of the postmodernist account of self-formation are MICHEL FOUCAULT, DISCIPLINE AND PUNISH: THE BIRTH OF THE PRISON (Alan Sheridan trans., Vintage Books 2d ed. 1995) (1977); and Michel Foucault, *Technologies of the Self*, *in* TECHNOLOGIES OF THE SELF: A SEMINAR WITH MICHEL FOUCAULT 16 (Luther H. Martin et al. eds., 1988). Important examples of the pragmatist approach include GEORGE H. MEAD, MIND, SELF, AND SOCIETY: FROM THE STANDPOINT OF A SOCIAL BEHAVIORIST (Charles W. Morris ed., Univ. of Chi. Press 1962) (1934); and JOHN DEWEY, EXPERIENCE AND NATURE (1925).

[13] *See generally, e.g.*, NICK CROSSLEY, THE SOCIAL BODY: HABIT, IDENTITY, AND DESIRE (2001); ELIZABETH GROSZ, VOLATILE BODIES: TOWARD A CORPOREAL FEMINISM (1994); DON IHDE, POSTPHENOMENOLOGY: ESSAYS IN THE POSTMODERN CONTEXT (1993).

[14] *See, e.g.*, COHEN, *supra* note 4; Daniel J. Solove, *Conceptualizing Privacy*, 90 CALIF. L. REV. 1087 (2002); Valerie Steeves, *Reclaiming the Social Value of Privacy*, *in* LESSONS FROM THE IDENTITY TRAIL: ANONYMITY, PRIVACY AND IDENTITY IN A NETWORKED SOCIETY 191 (Ian Kerr et al. eds., 2009).

[15] *See* Anita Allen, *Configuring the Networked Self: Shared Conceptions and Critiques*, CONCURRING OPINIONS (Mar. 6, 2012, 6:14 PM), http://www.concurringopinions.com/archives/2012/03/configuring-the-networked-self-shared-conceptions-and-critiques.html.

[16] *See, e.g.*, ALLEN, *supra* note 8; HELEN NISSENBAUM, PRIVACY IN CONTEXT (2010); David Matheson, *A Distributive Reductionism About the Right to Privacy*, 91 MONIST 108 (2008); Jeffrey H. Reiman, *Privacy, Intimacy, and Personhood*, 6 PHIL. & PUB. AFF. 26 (1976); Lisa M. Austin, Privacy, Shame, and the Anxieties of Identity (Jan. 1, 2012) (unpublished manuscript), *available at* http://ssrn.com/abstract=2061748.

A synthetic, postliberal approach to the problem of selfhood reveals a subjectivity that emerges gradually, in ways that are substantially constrained but not rigidly determined by social shaping. Emergent subjectivity is a byproduct of the ordinary, everyday behaviors of subjects who are situated within social and cultural landscapes. People are born into networks of relationships, practices, and beliefs, and over time they encounter and experiment with others, engaging in a diverse and ad hoc mix of practices that defies neat theoretical simplification.[17] In particular, the everyday practice of situated subjects does not conform to the idealized theoretical models preferred by liberal legal theorists, which revolve around the exercise of expressive or market liberty; it is messy, heterogeneous, and tactical. Most importantly, it is playful, and this is true in two different and equally important senses.[18] First, situated subjects exercise a deliberate, playful agency. Everyday practice can be enormously creative in ways that work around or push back against the institutional, cultural, and material constraints that people encounter. Second, the everyday practice of situated subjects exploits environmental serendipity: the unexpected encounters and juxtapositions that open new pathways for emergent subjectivity to explore. All of this means that processes of social and cultural construction do not automatically produce that caricature, the dominated postmodernist subject. Yet they are nonetheless extraordinarily important. Emergent subjectivity can evolve in ways that produce a robust sense of agency, supportive and resilient networks of relational ties, and critical independence of mind, but other results are also possible, depending on the nature of the constraints that are in place and on how tightly they bind.

I call this vision of selfhood a postliberal one because its relationship to liberalism requires something more difficult and much more productive than antagonism: a realistic appraisal of the liberal model's undeniable faults and equally undeniable virtues. Liberal selfhood has an important role to play within privacy theory, but that role is different from the one that most privacy scholars have assumed. The liberal self is an aspiration — an idealized model of identity formation that can be approached only incompletely, if at all. This does not mean that all of its attributes are equally attractive and worth pursuing. Certain features of liberal selfhood have been roundly and justifiably critiqued, most notably its abstraction from embodied reality and its

---

[17] *See* COHEN, *supra* note 4, at 50–57. *See generally* MICHEL DE CERTEAU, THE PRACTICE OF EVERYDAY LIFE (Steven Rendall trans., 1984); ANDREW PICKERING, THE MANGLE OF PRACTICE: TIME, AGENCY, AND SCIENCE (1995).

[18] For a more detailed discussion of the connection between everyday practice and play, see COHEN, *supra* note 4, at 53–57.

independence from relational ties.[19] But others — most notably the liberal self's capacity for critical independence of thought and judgment, its commitments to self-actualization and reason, and its aspiration to cosmopolitanism — are essential tools for identifying and pursuing the material and political conditions for self-fulfillment and more broadly for human flourishing.[20]

But here we must come back to privacy, for the development of critical subjectivity is a realistic goal only to the extent that privacy comes into play. Subjectivity is a function of the interplay between emergent selfhood and social shaping; privacy, which inheres in the interstices of social shaping, is what permits that interplay to occur. Privacy is not a fixed condition that can be distilled to an essential core, but rather "an interest in breathing room to engage in socially situated processes of boundary management."[21] It enables situated subjects to navigate within preexisting cultural and social matrices, creating spaces for the play and the work of self-making.

And once this point is established, privacy's dynamism becomes clear. Lack of privacy means reduced scope for self-making — along the lines of the liberal ideal, or along other lines. Privacy does not negate social shaping. "In a world with effective boundary management, however, there is play in the joints, and that is better than the alternative. . . . Privacy's goal, simply put, is to ensure that the development of subjectivity and the development of communal values do not proceed in lockstep."[22] Privacy will not always produce expressions of subjectivity that have social value, and here I mean expressly to leave open the question whether there might be particular types of privacy claims that do not merit protection or even respect.[23] Even so, privacy is one of the resources that situated subjects require to flourish.

---

[19] *See generally, e.g.*, N. KATHERINE HAYLES, HOW WE BECAME POSTHUMAN: VIRTUAL BODIES IN CYBERNETICS, LITERATURE, AND INFORMATICS (1999); JENNIFER NEDELSKY, LAW'S RELATIONS (2011).

[20] *See* MARTHA C. NUSSBAUM, WOMEN AND HUMAN DEVELOPMENT 59–70 (2000). *See generally* KWAME ANTHONY APPIAH, THE ETHICS OF IDENTITY (2005). I mean here more generally to ally myself with the theory of capabilities for human flourishing developed by Martha Nussbaum and Amartya Sen. *See, e.g.*, NUSSBAUM, *supra*, at 70–96; Amartya Sen, *Elements of a Theory of Human Rights*, 32 PHIL. & PUB. AFF. 315, 330–38 (2004); *see also* COHEN, *supra* note 4, at 21–24.

[21] COHEN, *supra* note 4, at 149.

[22] *Id.* at 150.

[23] *See, e.g.*, Whitney Phillips, *What an Academic Who Wrote Her Dissertation on Trolls Thinks of Violentacrez*, ATLANTIC (Oct. 15, 2012, 12:32 PM), http://www.theatlantic.com/technology/archive/2012/10/what-an-academic-who-wrote-her-dissertation-on-trolls-thinks-of-violentacrez/263631 (discussing the online subculture of anonymous trolling).

III. PERFECT TECHNOLOGIES OF JUSTICE? PRIVACY AND LIBERAL DEMOCRACY

If, as I have argued, the capacity for critical subjectivity shrinks in conditions of diminished privacy, what happens to the capacity for democratic self-government? Conditions of diminished privacy shrink the latter capacity as well, because they impair the practice of citizenship. But a liberal democratic society cannot sustain itself without citizens who possess the capacity for democratic self-government. A society that permits the unchecked ascendancy of surveillance infrastructures cannot hope to remain a liberal democracy. Under such conditions, liberal democracy as a form of government is replaced, gradually but surely, by a different form of government that I will call modulated democracy because it relies on a form of surveillance that operates by modulation. Modulation and modulated democracy are emerging as networked surveillance technologies take root within democratic societies characterized by advanced systems of informational capitalism. Citizens within modulated democracies — citizens who are subject to pervasively distributed surveillance and modulation by powerful commercial and political interests — increasingly will lack the ability to form and pursue meaningful agendas for human flourishing.

It is useful to begin by considering the relationship between citizenship and political and economic institutions. That institutions shape opportunities for the exercise of citizenship is, I think, an unremarkable proposition. Citizenship is more than a status. It is also a set of practices — voting, public debate, and so on — and so the scope for the practice of citizenship will be defined in part by the practices that existing institutions encourage, permit, or foreclose. Less often acknowledged is that institutions configure citizens, inculcating habits of mind and behavior that lend themselves more readily to certain types of practices than to others. Institutions shape not only the scope but also the capacity for citizenship. One of the lessons of American experiments in democracy building, beginning in the 1980s in the former Soviet Union and continuing most recently in Afghanistan and Iraq, is that democracy is difficult to jumpstart. Well-functioning state and market institutions cannot be built in the span of a grant-funded research project or a military campaign. Their rhythms and norms must be learned and then internalized, bringing into being the habits of mind and behavior that democratic citizenship requires.

Still absent from this equation is the mediating effect of networked information and communication technologies. Like the other artifacts that we use in our daily lives, networked information technologies mediate our relationship to the world around us. Processes of mediation are partly behavioral. The particular design features of our artifacts make some activities seem easier and more natural and others more

difficult, and these implicit behavioral templates, or affordances, encourage us to behave in certain ways rather than others.[24] But processes of mediation are also conceptual and heuristic. Our artifacts organize the world for us, subtly shaping the ways that we make sense of it. Over time we come to perceive the world through the lenses that our artifacts create.[25] For example, an automobile-club map and the step-by-step instructions uttered by an in-car GPS or the iPhone's Siri interface represent local geography in radically different ways. Intriguingly, there is evidence to suggest that over time the processes of mediation and configuration become deeply encoded in our neurobiology, producing individuals who are actually wired to think and act differently.[26]

Networked information technologies mediate our experiences of the world in ways directly related to both the practice of citizenship and the capacity for citizenship, and so they configure citizens as directly or even more directly than institutions do. The practice of citizenship requires access to information and to the various communities in which citizens claim membership. In the networked information society, those experiences are mediated by search engines, social networking platforms, and content formats. Search engines filter and rank search results, tailoring both the results and the accompanying advertising to what is known about the searcher and prioritizing results in ways that reflect popularity and advertising payments. Social networking platforms filter and systematize social and professional relationships according to their own logics. Content formats determine the material conditions of access to information — for example, whether a video file can be copied or manipulated, or whether a news forum permits reader comments. Each set of processes structures the practice of citizenship and also subtly molds network users' understanding of the surrounding world.[27] To an increasing degree, then, the capacity for democratic self-government is defined in part by what those technologies and other widely used technologies allow, and by exactly how they allow it.

Trajectories of technological development are not inevitable, and so it does not follow that technologies must configure citizens in a partic-

---

[24] *See* Bryan Pfaffenberger, *Social Anthropology of Technology*, 21 ANN. REV. ANTHROPOLOGY 491, 503 (1992).

[25] Longer versions of this argument appear in COHEN, *supra* note 4, at 46–50; and Julie E. Cohen, *Configuring the Networked Citizen*, *in* IMAGINING NEW LEGALITIES 129, 131–32 (Austin Sarat et al. eds., 2012). On the mediating function of artifacts, see generally PETER-PAUL VERBEEK, WHAT THINGS DO: PHILOSOPHICAL REFLECTIONS ON TECHNOLOGY, AGENCY, AND DESIGN (Robert P. Crease trans., 2005).

[26] *See generally* NICHOLAS CARR, THE SHALLOWS: WHAT THE INTERNET IS DOING TO OUR BRAINS (2010).

[27] *See* Cohen, *Configuring the Networked Citizen*, *supra* note 25, at 133–36.

ular way. Here, though, two developments are worth noting carefully. One is the trend toward seamless, invisible design of digital artifacts and interfaces. Prevailing best practices in design, bolstered in some cases by the operation of trade secrecy law, obscure the workings of network architectures. The shift to "black box" platforms for access and participation makes the processes of mediation more difficult to understand and therefore to contest.[28] The controversy over electronic voting is a case in point. Computer scientists and public interest advocates have identified persistent concerns about the security and integrity of digital voting platforms, but efforts to address those concerns have been obstructed by assertions of trade secrecy protection.[29] Efforts to generate more widespread public attention to electronic voting issues also have been hampered by the technical complexity of the subject matter. As a result of the shift to electronic voting, access to a core democratic capability increasingly is mediated in ways that only a minority of citizens can claim to understand.

The second development worth remarking is the increasing extent to which networked surveillance technologies and practices pervade everyday life. In literature and in the popular press, the idea of a surveillance society is habitually linked with totalitarian political systems. That equation is too simple, however: "[T]he surveillance society is better thought of as the outcome of modern organizational practices, businesses, government and the military than as a covert conspiracy. Surveillance may be viewed as progress towards efficient administration, in Max Weber's view, a benefit for the development of Western capitalism and the modern nation-state."[30] This description calls to mind Bruce Ackerman's evocative formulation of a just society's ideal (though unrealizable) instrumentality as a "perfect technology of justice."[31] Within systems of surveillance, efficient administration is a paramount form of justice. According to country rankings published

---

[28] *See* FRANK PASQUALE, THE BLACK BOX SOCIETY: TECHNOLOGIES OF REPUTATION, SEARCH, AND FINANCE (forthcoming 2013) (manuscript at 3–19) (on file with the Harvard Law School Library). *See generally* Frank Pasquale, *Restoring Transparency to Automated Authority*, 9 J. ON TELECOMM. & HIGH TECH. L. 235 (2011).

[29] On the technical vulnerabilities of electronic voting, see Andrew W. Appel, *Security Seals on Voting Machines: A Case Study*, 14 ACM TRANSACTIONS ON INFO. & SYS. SECURITY 18:1 (2011), *available at* http://delivery.acm.org/10.1145/2020000/2019603/a18-appel.pdf; Michael Agresta, *Will the Next Election Be Hacked?*, WALL ST. J., Aug. 18–19, 2012, at C2. On the invocation of trade secrecy, see Danielle Keats Citron, *Open Code Governance*, 2008 U. CHI. LEGAL F. 355, 361; Ricardo Alonso-Zaldivar, *E-Voting May Be Scarier than Hanging Chads*, L.A. TIMES, Nov. 3, 2006, at A18.

[30] KIRSTIE BALL ET AL., SURVEILLANCE STUDIES NETWORK, A REPORT ON THE SURVEILLANCE SOCIETY 1 (David Murakami Wood ed., 2006) [hereinafter REPORT ON THE SURVEILLANCE SOCIETY] (citing FROM MAX WEBER: ESSAYS IN SOCIOLOGY (H.H. Gerth & C. Wright Mills eds., 1964)).

[31] BRUCE A. ACKERMAN, SOCIAL JUSTICE IN THE LIBERAL STATE 21–23 (1980).

by Privacy International in 2007, the United States was an "endemic surveillance society," a distinction it shared with the United Kingdom, Russia, China, Malaysia, Thailand, Taiwan, and Singapore.[32]

Networked information technologies enable surveillance to become modulation. Surveillance may be defined generically as attention that is "purposeful, routine, systematic and focused."[33] Networked information technologies enable surveillant attention to become continuous, pervasively distributed, and persistent.[34] This in turn facilitates modulation: a set of processes in which the quality and content of surveillant attention is continually modified according to the subject's own behavior, sometimes in response to inputs from the subject but according to logics that ultimately are outside the subject's control.[35]

While modulation could be undertaken by the government, within systems of informational capitalism it is more typically and effectively undertaken by private actors. Following Manuel Castells, I use "informational capitalism" to refer to the alignment of capitalism as a mode of production with informationalism as a mode of development: "[c]apitalism is oriented toward profit-maximizing, that is, toward increasing the amount of surplus appropriated by capital on the basis

---

[32] *National Privacy Ranking 2007 — Leading Surveillance Societies Around the World*, PRIVACY INT'L, https://www.privacyinternational.org/sites/privacyinternational.org/files/file-downloads/phrcomp_sort_0.pdf (last visited Mar. 30, 2013). Privacy International develops its rankings using an index consisting of fourteen factors: constitutional protection; statutory protection; privacy enforcement; use of identity cards and biometrics; extent of data sharing; use of visual surveillance; use of communication interception; extent of communication data retention; extent of government access to data; extent of workplace monitoring; surveillance of medical events, financial transactions, and physical movement; border and transborder issues; leadership; and democratic safeguards. *Id.*

[33] REPORT ON THE SURVEILLANCE SOCIETY, *supra* note 30, at 4.

[34] For a more detailed typology, see Christian Fuchs et al., *Introduction: Internet and Surveillance*, *in* INTERNET AND SURVEILLANCE: THE CHALLENGES OF WEB 2.0 AND SOCIAL MEDIA 1, 16–19 (Christian Fuchs et al. eds., 2012).

[35] *See* GREG ELMER, PROFILING MACHINES: MAPPING THE PERSONAL INFORMATION ECONOMY 41–50 (2004); William Bogard, *Simulation and Post-Panopticism*, *in* ROUTLEDGE HANDBOOK OF SURVEILLANCE STUDIES 30, 32–33 (Kirstie Ball et al. eds., 2012). See generally GILLES DELEUZE, *Postscript on Control Societies*, *in* NEGOTIATIONS, 1972–1990 (Martin Joughin trans., 1995):

> [C]apitalism in its present form is no longer directed toward production, which is often transferred to remote parts of the Third World . . . . It's directed toward metaproduction. It no longer buys raw materials and no longer sells finished products: it buys finished products or assembles them from parts. What it seeks to sell is services, and what it seeks to buy, activities. . . . Markets are won by taking control rather than by establishing a discipline, by fixing rates rather than by reducing costs, by transforming products rather than by specializing production. . . . Marketing is now the instrument of social control and produces the arrogant breed who are our masters. Control is short-term and rapidly shifting, but at the same time continuous and unbounded, whereas discipline was long-term, infinite, and discontinuous. A man is no longer a man confined but a man in debt.

Id. at 181.

of the private control over the means of production and circulation," while "informationalism is oriented . . . toward the accumulation of knowledge and towards higher levels of complexity in information processing."[36] In the contemporary information economy, private-sector firms like Google, Facebook, and data broker Acxiom use flows of information about consumer behavior to target advertisements, search results, and other content. Advertisers and other client firms rely on the flows of information to construct pricing and risk management templates that maximize their ability to identify high-value consumers and to extract surplus from all consumers. Still other firms rely on flows of information to authenticate access to places (such as workplaces and gaming environments), services (such as banking and telecommunications), and networked information resources (such as software and databases). Information from and about consumers feeds into sophisticated systems of predictive analytics so that surveillant attention can be personalized more precisely and seamlessly. Government is an important secondary beneficiary of informational capitalism, routinely accessing and using flows of behavioral and communications data for its own purposes. The embedding of surveillance functionality within market and political institutions produces "surveillant assemblage[s]," in which information flows in circuits that serve the interests of powerful entities, both private and public.[37]

In the modulated society, surveillance is not heavy-handed; it is ordinary, and its ordinariness lends it extraordinary power. The surveillant assemblages of informational capitalism do not have as their purpose or effect the "normalized soul training" of the Orwellian nightmare.[38] They beckon with seductive appeal. Individual citizen-consumers willingly and actively participate in processes of modulation, seeking the benefits that increased personalization can bring. For favored consumers, these benefits may include price discounts, enhanced products and services, more convenient access to resources, and heightened social status.[39] Within surveillant assemblages, patterns of information flow are accompanied by discourses about why

---

[36] 1 MANUEL CASTELLS, THE INFORMATION AGE: THE RISE OF THE NETWORK SOCIETY 14–18 (1996).

[37] Kevin D. Haggerty & Richard V. Ericson, *The Surveillant Assemblage*, 51 BRIT. J. SOC. 605, 614–15 (2000).

[38] *Id.* at 615.

[39] For a detailed exploration of these processes, see generally MARK ANDREJEVIC, ISPY: SURVEILLANCE AND POWER IN THE INTERACTIVE ERA (2007). The discourses of personalization and convenience tend not to acknowledge that, for less favored consumers, the consequences of commercial profiling are quite different. *See* Seeta Peña Gangadharan, *Digital Inclusion and Data Profiling*, FIRST MONDAY (May 7, 2012), http://www.firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/3821/3199.

the patterns are natural and beneficial, and those discourses foster widespread internalization of the new norms of information flow.

For all of these reasons, a critique of surveillance as privacy invasion "does not do justice to the productive character of consumer surveillance."[40] Modulation is a mode of privacy invasion, but it is also a mode of knowledge production designed to produce a particular way of knowing and a mode of governance designed to produce a particular kind of subject. Its purpose is to produce tractable, predictable citizen-consumers whose preferred modes of self-determination play out along predictable and profit-generating trajectories. Yet to speak of networked processes of surveillance and modulation in the industrial-era vernacular, as systems for "manufacturing consent," would be too crude.[41] Rather, in a much more subtle process of continual feedback, stimuli are tailored to play to existing inclinations, nudging them in directions that align with profit-maximizing goals.[42] So too with political inclinations; particularly as search and social networking become more seamlessly integrated, networked citizen-consumers move within personalized "filter bubbles" that conform the information environment to their political and ideological commitments.[43] This is conducive to identifying and targeting particular political constituencies,[44] but not necessarily to fostering political dialogue among diverse constituencies in ways that might enable them to find common ground.

By these increasingly ordinary processes, both public and private regimes of surveillance and modulation diminish the capacity for democratic self-government. To be clear, I do not mean to suggest that surveillance is never necessary, nor that it is inevitably pernicious. Governments require some kinds of knowledge about people to govern effectively. I also want expressly to leave open the question whether national security imperatives might justify certain types of heightened surveillance. But in for a penny should not mean in for a pound. Citizens of the modulated society are not the same citizens that the liberal democratic political tradition assumes, nor do their modulated preferences even approximately resemble the independent decisions, formed

---

[40] Mark Andrejevic, *Exploitation in the Data Mine*, *in* INTERNET AND SURVEILLANCE, *supra* note 34, at 71, 73.

[41] The canonical reference is EDWARD S. HERMAN & NOAM CHOMSKY, MANUFACTURING CONSENT: THE POLITICAL ECONOMY OF THE MASS MEDIA (1988).

[42] *See* ANDREJEVIC, *supra* note 39, at 126–34.

[43] *See generally* ELI PARISER, THE FILTER BUBBLE: WHAT THE INTERNET IS HIDING FROM YOU (2011); KATHLEEN HALL JAMIESON & JOSEPH N. CAPPELLA, ECHO CHAMBER: RUSH LIMBAUGH AND THE CONSERVATIVE MEDIA ESTABLISHMENT 75–82 (2008); William Saletan, *Bubble Think: How to Escape a Partisan Echo Chamber*, SLATE (May 3, 2010, 8:45 AM), http://www.slate.com/articles/news_and_politics/frame_game/2010/05/bubble_think.html.

[44] *See, e.g.*, Charles Duhigg, *Campaigns Mine Personal Lives to Get Out Vote*, N.Y. TIMES, Oct. 14, 2012, at A1.

through robust and open debate, that liberal democracy requires to sustain and perfect itself. The modulated society is the consummate social and intellectual rheostat, continually adjusting the information environment to each individual's comfort level. Liberal democratic citizenship requires a certain amount of *dis*comfort — enough to motivate citizens to pursue improvements in the realization of political and social ideals. The modulated citizenry lacks the wherewithal and perhaps even the desire to practice this sort of citizenship.

If this sounds like science fiction, it shouldn't. Like the liberal self, liberal democracy has always been an ideal to be pursued and approximated. A polity's ability to approximate liberal democracy has both institutional and material preconditions. In the generations following the framing of the U.S. Constitution, those who sought to build a functioning liberal democracy had to contend with the gulf between liberalism's aspirations to egalitarianism and the concentration of political power in an entitled minority of white male property and slave owners. In the generations to come, those who seek to maintain a functioning liberal democracy will need to contend with the gulf between liberalism's aspirations to self-government by an informed and vigilant citizenry and the relatively blunted capacities of a modulated citizenry.

To put the point a different way, the liberal self and the liberal democratic society are symbiotic ideals. Their inevitably partial, imperfect realization requires habits of mind, of discourse, and of self-restraint that must be learned. Those are the very same habits that support a mature, critical subjectivity, and they require privacy to form. The institutions of modulated democracy, which systematically eradicate breathing space for dynamic privacy, deny both critical subjectivity and critical citizenship the opportunity to flourish. The liberal democratic society will cease to be a realistic aspiration unless serious attention is given to the conditions that produce (aspiring) liberal selves.

IV. THE END OF THEORY? PRIVACY, "BIG DATA," AND INNOVATION

Conditions of diminished privacy also impair the capacity to innovate. This is so both because innovation requires the capacity for critical perspective on one's environment and because innovation is not only about independence of mind. Innovation also requires room to tinker, and therefore thrives most fully in an environment that values and preserves spaces for tinkering. A society that permits the unchecked ascendancy of surveillance infrastructures, which dampen and modulate behavioral variability, cannot hope to maintain a vibrant tradition of cultural and technical innovation. Efforts to repackage pervasive surveillance as innovation — under the moniker "Big Data" — are better understood as efforts to enshrine the methods and values

of the modulated society at the heart of our system of knowledge production. The techniques of Big Data have important contributions to make to the scientific enterprise and to social welfare, but as engines of truth production about human subjects they deserve a long, hard second look.

An understanding of "innovation" as the absence of regulatory constraint features prominently in contemporary information policy discourse. The need to incentivize innovation is offered as the justification for strengthening proprietary control of intellectual goods and as the justification for regulating information networks lightly (if at all). In debates about information privacy, innovation is increasingly positioned as a justification for withholding data protection, and for looking the other way when privacy breaches appear to violate existing promises to consumers and regulators. Sometimes the opposition between privacy and innovation is explicit, but more often it is implicit in rhetoric that aligns innovation with unfettered information collection and processing.[45] Innovation then joins the list of values against which privacy must be balanced — and, of course, no one wants to go on record as opposing innovation. Confronted with asserted conflicts between privacy on the one hand and innovation and economic competitiveness on the other, regulators timidly opine that privacy harms result from "unexpected" disclosures of personal information and that more robust guarantees of notice and choice therefore may be needed to "build[] consumer trust in the marketplace."[46]

This simplistic view of the relationship between privacy and innovation is wrong. It fails to take into account either the nature of innovative practice or the dynamic function of privacy. Innovation does not follow an inevitable, linear arc to a predetermined end. It depends for its realization on innovative practice by situated subjects, and innovative practice is not linear; in Brett Frischmann's words, it is "mul-

---

[45] *See, e.g.*, *Balancing Privacy and Innovation*, *supra* note 1, at 13 ("And what happens when you follow the European privacy model and take information out of the information economy? . . . [R]evenues fall, innovation stalls, and you lose out to innovators who choose to work elsewhere."); *An Examination of Children's Privacy: New Technologies and the Children's Online Privacy Protection Act: Hearing Before the Subcomm. on Consumer Prot., Prod. Safety, & Ins. of the S. Comm. on Commerce, Sci., & Transp.*, 111th Cong. 49 (2010) (statement of Berin Szoka, Senior Fellow and Director, Center for Internet Freedom, The Progress & Freedom Foundation) (arguing that expanded privacy protection for children could "discourage innovation, limit choice, and raise prices for consumers"); FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS 7, 15, 26–28, 36 (2012) (summarizing comments received from affected industries); *FTC Cautioned Against Heavy Privacy Rules*, *supra* note 1, at 4 ("'Imposing burdensome privacy restrictions could limit Facebook's ability to innovate, making it harder for Facebook to compete in a constantly evolving industry,' the company said."); Nicklas Lundblad & Betsy Masiello, *Opt-in Dystopias*, 7 SCRIPTED 155 (2010), http://www.law.ed.ac.uk/ahrc/script-ed/vol7-1/lundblad.pdf.

[46] FED. TRADE COMM'N, *supra* note 45, at 7–9.

tidirectional, stochastic, [and] full of feedback loops."[47] External obstacles, whether material or regulatory, affect the feedback loops, but also represent opportunities; innovation emerges from the interplay between freedom and constraint. Innovative practice is threatened most directly when circumstances impose intellectual regimentation, prescribing orthodoxies and restricting the freedom to tinker. It thrives most fully when circumstances yield serendipitous encounters with new resources and ideas, and afford the intellectual and material breathing room to experiment with them.[48]

When the predicate conditions for innovation are described in this way, the problem with characterizing privacy as anti-innovation becomes clear: it is modulation, not privacy, that poses the greater threat to innovative practice. Regimes of pervasively distributed surveillance and modulation seek to mold individual preferences and behavior in ways that reduce the serendipity and the freedom to tinker on which innovation thrives. The suggestion that innovative activity will persist unchilled under conditions of pervasively distributed surveillance is simply silly; it derives rhetorical force from the cultural construct of the liberal subject, who can separate the act of creation from the fact of surveillance. As we have seen, though, that is an unsustainable fiction. The real, socially constructed subject responds to surveillance quite differently — which is, of course, exactly why government and commercial entities engage in it. Clearing the way for innovation requires clearing the way for innovative practice by real people. Innovative practice in turn requires breathing room for critical self-determination and physical spaces within which the everyday practice of tinkering can thrive.

There is, however, a new flavor of innovation on the scene: Big Data. "Big Data" is shorthand for the combination of a technology and a process. The technology is a configuration of information-processing hardware capable of sifting, sorting, and interrogating vast quantities of data in very short times. The process involves mining the data for patterns, distilling the patterns into predictive analytics, and applying the analytics to new data. Together, the technology and the process comprise a technique for converting data flows into a particular, highly

---

[47] BRETT M. FRISCHMANN, INFRASTRUCTURE: THE SOCIAL VALUE OF SHARED RESOURCES 272 (2012). On the origins and staying power of the linear model of innovation, see generally Benoît Godin, *The Linear Model of Innovation: The Historical Construction of an Analytical Framework*, 31 SCI., TECH. & HUM. VALUES 639 (2006).

[48] On the importance of serendipity and "flow" for creative and innovative practice, see generally TERESA M. AMABILE, CREATIVITY IN CONTEXT (1996); MIHALY CSIKSZENTMIHALYI, CREATIVITY: FLOW AND THE PSYCHOLOGY OF DISCOVERY AND INVENTION (1996); HOWARD GARDNER, CREATING MINDS (1993). *Cf.* PICKERING, *supra* note 17, at 21–24 (characterizing scientific innovation as the product of a "dialectic of resistance and accommodation," *id.* at 22–23).

data-intensive type of knowledge.[49] The technique of Big Data can be used to analyze data about the physical world — for example, climate or seismological data — or it can be used to analyze physical, transactional, and behavioral data about people. So used, it is vastly more nimble than old practices of category-driven profiling developed in the late twentieth century and now widely criticized.[50] According to its enthusiasts, Big Data will usher in a new era of knowledge production and innovation, producing enormous benefits to science and business alike. According to its critics, Big Data is profiling on steroids, unthinkably intrusive and eerily omniscient.

Big Data's claims to epistemological privilege stem from its asserted fidelity to reality at a very high level of detail. Its most avid enthusiasts do not paint it simply as an improvement in the state of the profiling art; rather, they claim that Big Data will eliminate the need for models altogether.[51] In place of predetermined and inevitably artificial categories, it will produce predictions and recommendations finely tailored to particular situations. Armed with enough data, researchers of all types will be able to jettison the post hoc, oversimple models through which they — and through them, we — have perceived the world in favor of reality, unfiltered. In the era of Big Data, we will have knowledge without visionaries. In the domain of information processing, we will have innovation without innovators, purged of the sloppiness, bias, and incompleteness that attends ordinary human endeavors. The always-on digital feedback processes of Big Data are highly attuned to individual variation, and therefore capable of making minute distinctions among individual subjects, but they generate and automatically refine their own analytic frameworks. Even those observers who do not explicitly subscribe to this understanding of Big Data offer tantalizing visions of improved understand-

---

[49] *See generally, e.g.*, Dave Feinleib, *The 3 I's of Big Data*, FORBES (July 9, 2012, 4:05 PM), http://www.forbes.com/sites/davefeinleib/2012/07/09/the-3-is-of-big-data; Jeff Kelly, *Big Data: Hadoop, Business Analytics and Beyond*, WIKIBON (Dec. 24, 2012, 9:58 AM), http://wikibon.org/wiki/v/Big_Data:_Hadoop,_Business_Analytics_and_Beyond.

[50] For a detailed analysis of category-driven profiling, see generally OSCAR H. GANDY, JR., THE PANOPTIC SORT: A POLITICAL ECONOMY OF PERSONAL INFORMATION (1993).

[51] *See, e.g.*, Chris Anderson, *The End of Theory: The Data Deluge Makes the Scientific Method Obsolete*, WIRED (June 23, 2008), http://www.wired.com/science/discoveries/magazine/16-07/pb_theory ("At the petabyte scale . . . [we] lose the tether of data as something that can be visualized in its totality."); *see also* ERIC TOPOL, THE CREATIVE DESTRUCTION OF MEDICINE 228 (2012) ("[W]e will arrive at a knowledge of individuals so fine-grained that we can speak of a science of individuality."); *Reinventing Society in the Wake of Big Data: A Conversation With Alex (Sandy) Pentland*, EDGE (Aug. 30, 2012), http://edge.org/conversation/reinventing-society-in-the-wake-of-big-data ("We're entering a new era of social physics, where it's the details of all the particles — the you and me — that actually determine the outcome.").

ing and innovative leaps in areas ranging from pandemic detection and drug design to traffic control and inventory management.[52]

To begin with, it is worth unpacking the atmospherics surrounding some of the more extreme claims about what Big Data promises. There is considerable irony in the spectacle of a technoculture that has long celebrated innovation as the ultimate expression of enlightened individualism seeking a modality for innovation that will transcend individual agency altogether. Irony compounds irony: some of the claims on behalf of Big Data, those framed in terms of a "singularity" waiting in our soon-to-be-realized future, sound quasi-religious, conjuring up the image of throngs of dyed-in-the-wool rationalists awaiting digital rapture.[53] To cultural historians, these claims likely have a familiar ring: they are expressions of the "technological sublime," a utopian (and singularly American) faith in the promise of better living through technology.[54] Reality lags predictably behind utopia, however, and so it is important to consider the ways in which Big Data as an enterprise is actually developing.

Considered more soberly, the claim that Big Data will eliminate the need for scientific modeling simply does not make sense. By this claim I do not mean to imply that the techniques that comprise Big Data lack value as tools for knowledge discovery, nor to deny that those techniques will sometimes represent radical improvements upon preexisting tools. To take just two examples, the application of predictive analytics to massive data sets will certainly enhance climatologists' understanding of weather patterns and improve epidemiologists' ability to understand and respond to public health problems. It is beyond serious question that the techniques that comprise Big Data offer vitally important strategies for promoting human flourishing in an increasingly complex, crowded, and interdependent world. But those techniques cannot themselves decide which questions to investigate, cannot instruct us how to place data flows and patterns in larger conceptual or normative perspective, and cannot tell us whether and when it might be fair and just to limit data processing in the service of other values. These shortcomings mean that Big Data cannot replace either human-driven modeling or the prior decisions about direction and

---

[52] *See, e.g.*, Omer Tene & Jules Polonetsky, *Privacy in the Age of Big Data: A Time for Big Decisions*, 64 STAN. L. REV. ONLINE 63, 63–65 (2012); Omer Tene & Jules Polonetsky, *Big Data for All: Privacy and User Control in the Age of Analytics*, 11 NW. J. TECH. & INTELL. PROP. (forthcoming 2013).

[53] *See* Brandon Keim, *Will the Singularity Make Us Happier?*, WIRED (May 30, 2008, 11:53 AM), http://www.wired.com/wiredscience/2008/05/will-the-singul.

[54] *See generally* DAVID E. NYE, AMERICAN TECHNOLOGICAL SUBLIME (1994); VINCENT MOSCO, THE DIGITAL SUBLIME (2004).

scope that set the substantive and ethical parameters for particular programs of investigation.

Here it is worth noting that the enthusiasm for Big Data has another set of cultural antecedents that is less immediately obvious, but ultimately more troubling. As Wall Street's flavor of the month, Big Data stands in a long and undistinguished tradition. The "smartest guys in the room"[55] no longer work for Enron, Lehman Brothers, or AIG; now they work for Google or Target or Acxiom, pursuing the holy grail of knowing customers better than they know themselves. Features in the *Wall Street Journal* and the *Economist* pay homage to the heady combination of computing horsepower and technical machismo that the quest demands.[56] Personalization is the new religion of the information society, and the quant jocks of Big Data are its high priests. The skeptic's questions about downside risks go unanswered, and often unasked.

Innovation is never a neutral quantity. Technologies and artifacts are shaped by the values, priorities, and assumptions of their developers, and often by those of their users as well. Of course, many technologies are designed or refined with particular goals in mind, but here I am referring to a different and less deliberate shaping process, through which artifacts come to reflect and reproduce beliefs about the types of functions and ways of living and working that are important.[57] To return to a previous example, the design of an in-car GPS interface prioritizes getting from point A to point B most efficiently. The design of a child's car seat prioritizes modularity and affordability over compact size; therefore, it promotes safety but not the purchase of smaller, more fuel-efficient cars. The techniques of Big Data are no exception to this rule of cultural constructedness.

In particular, I want to highlight three distinct but mutually reinforcing problems: three ways in which the shift to Big Data now playing out within the particular context of the system of informational capitalism seems likely to reinforce certain values, and favor certain

---

[55] BETHANY MCLEAN & PETER ELKIND, THE SMARTEST GUYS IN THE ROOM: THE AMAZING RISE AND SCANDALOUS FALL OF ENRON (2003); *see also* ENRON: THE SMARTEST GUYS IN THE ROOM (Magnolia Pictures 2005).

[56] *See, e.g.*, Dennis K. Berman, *The Game: So, What's Your Algorithm?*, WALL ST. J., Jan. 4, 2012, at B1; *Data, Data Everywhere*, ECONOMIST, Feb. 27, 2010 (Data, Data Everywhere: A Special Report on Managing Information), at 1; *A Different Game*, ECONOMIST, Feb. 27, 2010 (Data, Data Everywhere: A Special Report on Managing Information), at 4; *A Golden Vein*, ECONOMIST, June 12, 2004 (Technology Quarterly), at 18; Mark P. Mills & Julio M. Ottino, *The Coming Tech-Led Boom*, WALL ST. J., Jan. 30, 2012, at A15.

[57] *See generally* THE SOCIAL SHAPING OF TECHNOLOGY (Donald MacKenzie & Judy Wajcman eds., 2d ed. 1999); Sally Wyatt, *Technological Determinism Is Dead; Long Live Technological Determinism*, *in* THE HANDBOOK OF SCIENCE AND TECHNOLOGY STUDIES 165 (Edward J. Hackett et al. eds., 3d ed. 2008).

kinds of knowledge, over others. The first problem concerns hidden research agendas. Big Data may seem to update and improve upon traditional scientific modeling because its investigations are both open-ended and ongoing. Such investigations do not conform to the idea of the scientific research program as a series of limited data collections for the purpose of testing and possibly falsifying a particular hypothesis.[58] Big Data's relative advantage (according to some) is its ability to make sense, in real time, of an ever-changing data landscape. Decisions about research agendas need not be explicit, however. The research agendas that drive Big Data will be those of the entities that deploy it. It is at this point that a more general principle of falsifiability begins to matter. Even within academic computational science, attaining the transparency required to confirm or falsify results is Big Data's Achilles' heel; observers have begun to point to a "credibility crisis" that derives from inadequate disclosure of data sets and methods.[59] Big Data in the private sector neither pretends nor aspires to transparency; research agendas and data sets are typically kept secret, as are the analytics that underpin them.

The second problem concerns underlying ideology. Big Data is the ultimate expression of a mode of rationality that equates information with truth and more information with more truth, and that denies the possibility that information processing designed simply to identify "patterns" might be systematically infused with a particular ideology. Those core premises are deeply entrenched within American intellectual culture. Even when private-sector research agendas are uncovered and become the subjects of investigation and critique in the pages of *The Atlantic* and the *New York Times Magazine*,[60] we seem unable to challenge the techniques of Big Data as knowledge-production practices. But the denial of ideology is itself an ideological position. Information is never just information: even pattern identification is informed by values about what makes a pattern and why, and why the

---

[58] That understanding of the scientific method is simplistic. On the scientific method and scientific modeling, see generally DANIELA M. BAILER-JONES, SCIENTIFIC MODELS IN PHILOSOPHY OF SCIENCE (2009); SCIENCE RULES: A HISTORICAL INTRODUCTION TO SCIENTIFIC METHODS (Peter Achinstein ed., 2004). For a provocative exploration of the mismatch between Big Data and the traditional understanding of the scientific method, see *Reinventing Society in the Wake of Big Data: A Conversation With Alex (Sandy) Pentland*, *supra* note 51.

[59] Victoria Stodden, *The Credibility Crisis in Computational Science* (Feb. 1, 2012), http://academiccommons.columbia.edu/download/fedora_content/download/ac:147758/CONTENT/BerkeleyFeb2012-STODDEN.pdf; *see also* Yale Law Sch. Roundtable on Data & Code Sharing, *Reproducible Research: Addressing the Need for Data and Code Sharing in Computational Social Science*, COMPUTING SCI. & ENGINEERING 8, 9 (Sept./Oct. 2012).

[60] *See, e.g.*, Charles Duhigg, *Psst, You in Aisle 5*, N.Y. TIMES, Feb. 19, 2012, § 6 (Magazine), at 30; William F. Pewen, *Protecting Our Civil Rights in the Era of Digital Health*, ATLANTIC (Aug. 2, 2012, 11:09 AM), http://www.theatlantic.com/health/archive/2012/08/protecting-our-civil-rights-in-the-era-of-digital-health/260343.

pattern in question is worth noting. Pattern identification also is informed by both content and categorization biases in the databases of origin; thus, for example, the Facebook data set has particular demographics and reflects particular beliefs about what makes someone a "friend." Big Data does not interrogate those choices; it does not need to. Big Data is the intellectual engine of the modulated society. Its techniques are techniques for locating and extracting consumer surplus and for managing, allocating, and pricing risk, and it takes data sets at face value. But the values of predictive rationality and risk management are *values*, and they are the values with which serious critics of Big Data need to contend.

The third problem is, once again, the problem of constructed subjectivity, and more specifically the problem of subjectivity constructed in the service of the self-interested agendas of powerful economic actors. The integrity of behavioral and preference data is a longstanding concern within social science research, and this concern has led to the development of elaborate techniques of research design to minimize distortion. Big Data attacks the problem of data integrity from a different direction by gathering behavioral data at the source (and often without the subjects' knowledge). Even when it operates unobserved, however, Big Data cannot neutralize the problem of constructed subjectivity, and instead is more likely both to exacerbate the problem and to insulate it from public scrutiny. The techniques of Big Data subject individuals to predictive judgments about their preferences, and the process of modulation also shapes and produces those preferences. The result is "computational social science" in the wild, a fast-moving and essentially unregulated process of experimentation on unsuspecting populations.[61] Big Data's practitioners are never "just watching." And here informational capitalism's interlinked preferences for consumer surplus extraction and risk management can be expected to move subjectivity in predictably path-dependent directions.[62]

By now it should be apparent that there are important procedural and ethical objections to some of the most common applications of Big Data. As deployed by commercial entities, Big Data represents the de facto privatization of human subjects research, without the procedural and ethical safeguards that traditionally have been required. Population studies using the techniques of Big Data typically proceed without

---

[61] Andre Oboler, Kristopher Welsh & Lito Cruz, *The Danger of Big Data: Social Media as Computational Social Science*, FIRST MONDAY (July 2, 2012), http://www.firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/3993/3269.

[62] On the relationship between prediction and risk management, see Ian Kerr, *Prediction, Preemption, Presumption: The Path of Law After the Computational Turn*, *in* PRIVACY, DUE PROCESS, AND THE COMPUTATIONAL TURN 87, 98–103 (Mireille Hildebrandt & Katja De Vries eds., forthcoming May 2013).

the sorts of controls that might be instituted by, for example, an institutional review board.[63] I tend to think this is a very bad idea. At minimum, it should be uncontroversial to suggest that these issues require further study.

Other objections are more subtle, and this brings us back to privacy. As already noted, privacy is increasingly cast as the spoiler in this tale, the obstacle to the triumphant march of predictive rationalism. Privacy scholars and advocates have not fully teased out the implications of this positioning, but they are dire: if information processing is rational, then anything that disrupts information processing, including privacy protection, is presumptively irrational. In the long run, I think that a strategy of avoidance on this point is a mistake; the implicit charge of irrationality must be answered. I have argued elsewhere that this characterization of privacy misses the mark. A commitment to privacy expresses a different kind of "sound reason" that we might choose to value — one that prizes serendipity as well as predictability and idiosyncrasy as well as assimilation.[64]

The distinction between predictive rationalism and reason directs our attention to the quality of the innovation Big Data seems likely to produce, and to the sorts of innovation most likely to be lost. Even if Big Data did not continually alter its own operands, it would not operate in a vacuum. It is a mistake to think of the techniques of Big Data as simply adding to the amount of information circulating within society. The valorization of predictive rationality and risk management inevitably displaces other kinds of knowledge that might be generated instead. Stimuli tailored to consumptive preferences crowd out other ways in which preferences and self-knowledge might be expressed, and also crowd out other kinds of motivators — altruism, empathy, and so on — that might spur innovation in different directions.[65] In a consumption-driven economy, the innovations that emerge and find favor will be those that fulfill consumption-driven needs. Contemporary applications of Big Data extend beyond marketing and advertising to core social and cultural functions, including the study of intellectual preferences and the delivery of higher education.[66] Systematizing those functions according to the dictates of predictive rationality threatens important social values. It crowds out the ability

---

63 *See generally* 45 C.F.R. §§ 46.101–.505 (2011); Lauren B. Solberg, *Regulating Human Subjects Research in the Information Age: Data Mining on Social Networking Sites*, 39 N. KY. L. REV. 327 (2012).

64 *See generally* Julie E. Cohen, *Irrational Privacy?*, 10 J. TELECOMM. & HIGH TECH. L. 241, 245–48 (2012).

65 *See generally* MICHAEL J. SANDEL, WHAT MONEY CAN'T BUY: THE MORAL LIMITS OF MARKETS (2012).

66 Marc Parry, *Please Be eAdvised*, N.Y. TIMES, July 22, 2012, at ED24.

to form and pursue other kinds of agendas for human flourishing, which is indispensable both to maintaining a vital, dynamic society and to pursuing a more just one.

In short, privacy is important both because it promotes innovative practice and because it promotes particular kinds of innovation that are extraordinarily important. The human innovative drive is both unpredictable and robust, but it does not follow that all environments are equally favorable to innovation or that all environments will produce the same kinds of innovation. If privacy and serendipity are critical to innovation — by which I mean critical both to the likelihood that innovation will occur and to the substance of that innovation — there is reason to worry when privacy is squeezed to the margins and when the pathways of serendipity are disrupted and rearranged to serve more linear, commercial imperatives. Environments that disfavor critical independence of mind and that discourage the kinds of tinkering and behavioral variation out of which innovation emerges will, over time, predictably and systematically disfavor innovation of all types. Environments designed to promote consumptive and profit-maximizing choices will systematically disfavor innovations designed to promote other values. The modulated society is dedicated to prediction but not necessarily to understanding or to advancing human material, intellectual, and political well-being. Data processing offers important benefits, but so does privacy. A healthy society needs both.

V. "MIND THE GAPS": FROM PRIVACY GOVERNANCE TO PRIVACY PROTECTION

Privacy rights protect individuals, but to understand privacy simply as an individual right is a mistake. The ability to have, maintain, and manage privacy depends heavily on the attributes of one's social, material, and informational environment. Recall that privacy in the dynamic sense is "an interest in breathing room to engage in socially situated processes of boundary management."[67] That interest has distinct structural entailments that efforts to design effective legal protection for privacy must acknowledge. In addition, privacy does not only protect individuals. Privacy furthers fundamental public policy goals relating to liberal democratic citizenship, innovation, and human flourishing, and those purposes must be taken into account when making privacy policy. The paradigm of "new privacy governance" that has been evolving within the U.S. legal system is unlikely to serve individual or public interests in privacy well, because it is rooted in a regulatory ideology that systematically downplays the need to hold market

[67] COHEN, *supra* note 4, at 149.

actors accountable for harms to the public interest. Effective privacy protection must target the qualities of seamlessness and opacity that together enable modulation.

Contemporary information privacy policy in the U.S. sits at the intersection of two ongoing conversations about the future of regulation in the networked information era. The first conversation concerns the appropriate uses of information architectures to bolster regulatory strategies. For the most part, that discussion has been structured by the taxonomy developed by Lawrence Lessig, which classifies "code" as one of four principal regulatory modalities, alongside law, markets, and norms.[68] The second conversation that informs privacy regulation concerns the appropriate division of regulatory authority in an era of economic and technical complexity. That conversation has produced a regulatory paradigm known as the "new governance," which favors reconfiguration of the public-private relationship in regulation and, often, the devolution of regulatory authority to private entities or public-private partnerships.[69] In the domain of information law and policy, the intersection of the four-modalities taxonomy with the new governance has produced a regulatory discourse with a technocratic flavor and a neoliberal ethic: "Descriptive accounts of regulation everywhere around us — in markets, in norms, and in 'code' — are increasingly conjoined with normative claims about the relative efficacy of privatized regulation through cooperative standard-setting, licensing of compliant implementations, joint ventures, and other collaborative activities by market participants."[70]

Privacy regulators operating within limited statutory grants of jurisdiction have embraced the new governance with enthusiasm. The Federal Trade Commission in particular has taken a leading role in shaping the new privacy governance, convening roundtables of "stakeholders" to identify best practices in personal information processing and exerting its enforcement authority principally via consent decrees negotiated with firms like Google and Facebook.[71] Privacy scholars have been more cautious about implementation but have applied themselves with a will to the task of reimagining privacy regulation through the new governance lens.[72]

---

[68] LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 86–95 (1999).

[69] *See generally* Jody Freeman, *The Private Role in Public Governance*, 75 N.Y.U. L. REV. 543 (2000); Orly Lobel, *The Renew Deal: The Fall of Regulation and the Rise of Governance in Contemporary Legal Thought*, 89 MINN. L. REV. 342 (2004).

[70] Cohen, *Configuring the Networked Citizen*, *supra* note 25, at 140–41.

[71] *See, e.g.*, Facebook, Inc., No. 092 3184 (Fed. Trade Comm'n Nov. 29, 2011); Google Inc., No. 102-3136 (Fed. Trade Comm'n Oct. 13, 2011); FED. TRADE COMM'N, *supra* note 45.

[72] *See, e.g.*, Kenneth A. Bamberger & Deirdre K. Mulligan, *New Governance, Chief Privacy Officers, and the Corporate Management of Information Privacy in the United States: An Initial Inquiry*, 33 LAW & POL'Y 477, 478–79 (2011); Kenneth A. Bamberger & Deirdre K. Mulligan,

The cautious, technocratic approach embodied in the new privacy governance, and the ambivalent regulatory response to corporate "privacy practices" that it has engendered, are the latest chapter in an ongoing romance between lawyers and techniques for processing and managing information. When such techniques are envisioned as neutral instrumentalities for pursuing more perfect social welfare, it is difficult to subject them to critical scrutiny. Ian Kerr traces this disinclination back to the influential writings of Oliver Wendell Holmes, Jr., who in 1897 famously opined that "the man of the future is the man of statistics."[73] Faith in the redemptive power of information technologies persists even when the appropriate tools are unavailable. Writing in 1980, Ackerman defended liberal democratic principles and institutions as a second-best solution to the impossible problem of reconciling competing and incommensurable goods, necessary because the best solution — a "perfect technology of justice" — did not exist.[74] In his 2005 paean to Big Data, Ackerman's colleague Ian Ayres is more optimistic, envisioning pattern recognition and predictive analytics as routes toward more perfectly enlightened decisionmaking about a wide variety of problems.[75]

The new privacy governance also has a politics that has been relatively resistant to critical scrutiny. As a way of joining the issue, I want to single out two interventions in the regulatory debate about networked information technologies that are noteworthy both for their prescience about the risks of modulation and for the way their reception in scholarly and policy circles highlights pathologies within the new governance paradigm. The first is Mark Tushnet's early critique of the four-modalities taxonomy, which worried that the taxonomy and the behavioral-control approach to regulation that it exemplifies could become way stations on the route to totalitarianism.[76] That worry met with a deafening silence; it is cited almost nowhere in the cyberlaw literature. In part this may be because Tushnet did not himself choose to pursue the project, but I think the primary reason is that at a moment when scholars and pundits hailed networked information technologies as the crown jewels of a democratic, capitalist political economy, the whiff of sulfur simply did not register. The second intervention is

---

Privacy on the Books and on the Ground, 63 STAN. L. REV. 247, 308–09 (2011); Viktor Mayer-Schönberger, *Beyond Privacy, Beyond Rights — Toward a "Systems" Theory of Information Governance*, 98 CALIF. L. REV. 1853, 1859–61 (2010).

[73] *See* Kerr, *supra* note 62, at 87 (quoting Oliver Wendell Holmes, Jr., *The Path of the Law*, 10 HARV. L. REV. 457, 469 (1897)).

[74] ACKERMAN, *supra* note 31, at 19–30.

[75] IAN AYRES, SUPER CRUNCHERS: WHY THINKING-BY-NUMBERS IS THE NEW WAY TO BE SMART (2007).

[76] Mark Tushnet, *"Everything Old Is New Again": Early Reflections on the "New Chicago School,"* 1998 WIS. L. REV. 579.

Frank Pasquale's proposal for federal regulation of neutrality in online search, which took aim directly at the free-market optimism that has animated so much thinking about information law and policy.[77] This proposal, styled not as a general warning but rather as a call for concrete regulatory action, has sparked intense criticism. Yet opponents of search engine regulation have seemed almost willfully blind to the thrust of Pasquale's critique, which has to do with the role of technical opacity in producing and reinforcing modulation.[78]

To consider the promise and potential of networked information technologies in the abstract without taking into account the ways in which they are deployed to produce modulation is, of course, to miss the point. That tendency reflects the deeply neoliberal philosophy that animates the new governance. New governance initiatives and rhetoric express what Jodi Short calls the "paranoid style" in regulatory reform: an intense worry about the risks of state coercion and bumbling, combined with relative insensitivity to the ramifications of private power, which produces "a regulatory reform discourse that is antithetical to the very idea of government regulation."[79] The politics of modulation is not a totalitarian politics. It is a politics that originates in the new governance paradigm's blind spot, in the concentrations of private economic and informational power that characterize informational capitalism.

For exactly these reasons, the new privacy governance is particularly ill-equipped to respond effectively to emerging practices of modulation. Its emphasis on privatized regulation and control of information flows via notice and choice reinforces precisely those aspects of modulation that are most troubling and most intractable. More precise modulation of information flows, aided by better-informed input from consumers, will not provide more privacy or better privacy. If privacy regulation is to provide effective shelter for socially situated processes of boundary management, we will need to acknowledge that privacy is the opposite of modulation and can exist only to the extent that processes of modulation are gap-ridden, transparent, and incomplete. A regulatory agenda for effective privacy protection will comprise

---

[77] *See* Frank Pasquale, *Beyond Innovation and Competition: The Need for Qualified Transparency in Internet Intermediaries*, 104 NW. U. L. REV. 105 (2010).

[78] *See, e.g.*, EUGENE VOLOKH & DONALD M. FALK, FIRST AMENDMENT PROTECTION FOR SEARCH ENGINE SEARCH RESULTS (2012), *available at* http://www.volokh.com/wp-content/uploads/2012/05/SearchEngineFirstAmendment.pdf; Eric Goldman, *Search Engine Bias and the Demise of Search Engine Utopianism*, 8 YALE J.L. & TECH. 188 (2006); Ryan Singel, Times *Case for Gov Regulation of Google Search Is Weak*, WIRED (July 16, 2010, 3:35 PM), http://www.wired.com/business/2010/07/nyt-google-regulation; Berin Szoka & Adam Thierer, *Just Say No to Ma Bell–Era Net Neutrality Regulation*, CNET (Aug. 11, 2010, 10:00 AM), http://news.cnet.com/8301-13578_3-20013262-38.html.

[79] Jodi L. Short, *The Paranoid Style in Regulatory Reform*, 63 HASTINGS L.J. 633, 635 (2012).

legal and architectural strategies for restraining code's perfectionist tendencies.

The devolution of regulatory authority over secret and logically opaque information processing practices also will not provide more privacy or better privacy. Protection against government surveillance is necessary if we are to avoid an Orwellian surveillance society, but it is neither a necessary nor a sufficient condition for avoiding the modulated society. The capacity for citizenship and the capacity for innovative practice depend importantly on the scope and reach of private-sector information processing. Effective privacy protection requires regulatory scrutiny of information processing activity on both sides of the public-private divide, and must include strategies for exposing networked processes of modulation to adequate public scrutiny.

The implications of this analysis for the design of effective privacy protection are far reaching and deserve far more sustained exploration than the format of this Symposium permits. Here I will simply sketch three of the most significant strategies for meaningful regulatory reform.

First, the interstitial character of privacy suggests a need to rethink the conception of due process as individualized decisionmaking. Privacy scholars and philosophers of technology have begun to question whether information processing practices that subject individuals to predictive and effectively preemptive judgments impair due process guarantees.[80] In the era of Big Data, the most individualized judgments are not necessarily the most dignifying. Due process in the era of comprehensive, preemptive computation may entail limits on fine-grained personalization in a range of public administrative processes. While it might seem tempting, for example, to calibrate disability benefits based on the precise level of need, or to engage in real-time monitoring of Medicaid recipients' food purchases to supervise nutritional choices, a liberal democratic society cannot simply deploy surveillance technologies to close the gap unfilled and unfillable by perfect technologies of justice.

Second and relatedly, effective protection for dynamic privacy requires affirmative measures designed to preserve and widen interstitial spaces within information processing practices on both sides of the public-private divide. Adequate breathing room for personal boundary management exists when legal, technical, and commercial architectures are characterized by a condition that I have called semantic discontinuity.[81] Semantic discontinuity is "the opposite of seamlessness: it

---

[80] *See* Kerr, *supra* note 62, at 103–08; *see also* Danielle Keats Citron, *Technological Due Process*, 85 WASH. U. L. REV. 1249, 1305–08 (2008).

[81] *See* COHEN, *supra* note 4, at 239–41, 248–66.

is a function of interstitial complexity within the institutional and technical frameworks that define information rights and obligations and establish protocols for information collection, storage, processing, and exchange."[82] Semantic discontinuity helps to separate contexts from one another, thereby preserving breathing room for personal boundary management and for the play of everyday practice. It is a condition that we should not lightly leave behind. A regulatory agenda for effective privacy protection should include the development of criteria for assessing semantic discontinuity and strategies for creating and maintaining adequate baseline levels.

Finally, effective privacy protection requires adequate levels of operational transparency about information processing practices.[83] The power of modulation derives partly from its precision, but partly from its operational opacity. Its engineers exert enormous power to shape the nature of innovative activity and the direction of public debate, yet they are not systematically held accountable to the public, and they should be. The need for accountability suggests more careful attention to the design of ostensibly technical processes from the outset; devolving regulatory and standard-setting authority to industry consortia, as the new governance model dictates, simply will not do. It also suggests that both regulators and designers of networked digital artifacts and interfaces should experiment with ways of disrupting the comfort zones produced by processes of modulation, drawing attention to their existence, and providing individual citizens with the resources to interrogate modulation's logics and effects.

VI. CONCLUSION

Writing in 1980, when the Cold War was still ongoing, political scientist and philosopher of technology Langdon Winner posed the question whether technologies can ever be said to have an inherent

---

[82] *Id.* at 239. The European movement for a "right to be forgotten" serves similar ends, but semantic discontinuity can be conceptualized more generally as a right to prevent precisely targeted individualization and continuous modulation. On the right to be forgotten, see *Commission Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation)*, at 9, COM (2012) 11 final (Jan. 25, 2012); Meg Leta Ambrose & Jef Ausloos, *The Right to be Forgotten Across the Pond*, 3 J. INFO. POL'Y 1, 11–14 (2013), http://jip.vmhost.psu.edu/ojs/index.php/jip/article/view/119/68; Lilian Mitrou & Maria Karyda, EU's Data Protection Reform and the Right to Be Forgotten — A Legal Response to a Technological Change? 10–13 (Oct. 22, 2012) (unpublished manuscript), *available at* http://ssrn.com/abstract=2165245.

[83] For more detailed versions of this argument, see COHEN, *supra* note 4, at 234–39, and Cohen, *supra* note 25, at 149–50; see also Pasquale, *supra* note 77, at 166.

politics.[84] He argued that although most technologies become imbued with politics as part of the process of their development, some do have a more determinate politics that flows from their compatibility with particular political arrangements. Networked information technologies are protean, and thus might seem an odd candidate for designation as inherently political. And yet all information flows reduce to bits, and all networked digital technologies possess at least the capacity for modulation. One might conclude that the inherently political character of networked information technologies is thus very much an open question. Yet it is closer to the truth, I think, to understand modulation from a perspective that emphasizes economic (as opposed to technological) determinism: a variant of materialism that underscores the dictates of the regime of political economy within which networked information technologies have emerged.[85]

What is certain is that privacy is important and urgently in need of preservation, and that current regulatory strategies seem unlikely to prove up to the task. Imbuing our networked information technologies with a different politics will require both the vision to appreciate privacy's dynamism and the will to think creatively about preserving it.

---

[84] LANGDON WINNER, THE WHALE AND THE REACTOR: A SEARCH FOR LIMITS IN AN AGE OF HIGH TECHNOLOGY 29–39 (1986).

[85] *See* Wyatt, *supra* note 57, at 168.