2012

Configuring the Networked Citizen

Julie E. Cohen
Georgetown University Law Center, jec@law.georgetown.edu

Originally published in Austin Sarat, Lawrence Douglas, and Martha Merrill Umphrey, eds., *Imagining New Legalities: Privacy and Its Possibilities in the 21st Century* (Stanford, CA: Stanford University Press, 2012), 129-53. © 2012 by the Board of Trustees of the Leland Stanford Jr. University.

Configuring the Networked Citizen in IMAGINING NEW LEGALITIES: PRIVACY AND ITS POSSIBILITIES IN THE 21st CENTURY (Austin Sarat, Lawrence Douglas & Martha Merrill Umphrey, eds., Stanford, Cal.: Stanford University Press 2012)

Originally published in Austin Sarat, Lawrence Douglas, and Martha Merrill Umphrey, eds., *Imagining New Legalities: Privacy and Its Possibilities in the 21st Century* (Stanford, CA: Stanford University Press, 2012), 129-53. © 2012 by the Board of Trustees of the Leland Stanford Jr. University.

Configuring the Networked Citizen

Julie E. Cohen

Among legal scholars of technology, it has become commonplace to acknowledge that the design of networked information technologies has regulatory effects. 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.[1] As a result of that framing, questions about the applicability of constitutional protections to technical decisions have taken center stage in legal and policy debates. Some scholars have pondered whether digital architectures unacceptably constrain fundamental liberties, and what "public" design obligations might follow from such a conclusion. Others have argued that code belongs firmly on the "private" side of the public/private divide because it originates in the innovative activity of private actors.

In a forthcoming book, I argue that the project of situating code within one or another part of the familiar constitutional landscape too often distracts legal scholars from more important questions about the quality of the regulation that networked digital architectures produce.[2] The gradual, inexorable embedding of networked information technologies has the potential to alter, in largely invisible ways, the interrelated processes of subject formation and culture formation. Within legal scholarship, the prevailing conceptions of subjectivity tend to be highly individualistic, oriented around the activities of speech and voluntary affiliation. Subjectivity also tends to be understood as definitionally independent of "culture." Yet subjectivity is importantly collective, formed by the substrate within which individuality emerges. People form their conceptions of the good in part by reading, listening, and watching—by engaging with the products of a common culture—and by interacting with one another. Those activities are socially and culturally mediated, shaped by the preexisting communities into which individuals are born and within which they develop. They are also technically mediated, shaped by the artifacts that individuals encounter in common use.

The social and cultural patterns that mediate the activities of self-constitution are being reconfigured by the pervasive adoption of technical protocols and services that manage the activities of content delivery, search, and social interaction. In developed countries, a broad cross-section of the population routinely uses networked information technologies and communications devices in hundreds of mundane, unremarkable ways. We search for information, communicate with each other, and gain access to networked resources and services. For the most part, as long as our devices and technologies work as expected, we give little thought to how they work; those questions are understood to be "technical" questions. Such questions are better characterized as sociotechnical. As networked digital architectures increasingly mediate the ordinary processes of everyday life, they catalyze gradual yet fundamental social and cultural change.

This chapter considers two interrelated questions that flow from understanding sociotechnical change as (re)configuring networked subjects. First, it revisits the way that legal and policy debates locate networked information technologies with respect to the public/private divide. The design of networked information technologies and communications devices is conventionally treated as a private matter; indeed, that designation has been the principal stumbling block encountered by constitutional theorists of technology. The classification of "code" as presumptively private has effects that reach beyond debates about the scope of constitutional guarantees, shaping views about the extent to which regulation of technical design decisions is normatively desirable. This chapter reexamines that discursive process, using lenses supplied by literatures on third-party liability and governance. Second, this chapter considers the relationship between sociotechnical change and understandings of citizenship. The ways that people think, form beliefs, and interact with one another are centrally relevant to the sorts of citizens that they become. The gradual embedding of networked information technologies into the practice of everyday life therefore has important implications for both the meaning and the practice of citizenship in the emerging networked information society. If design decisions are neither "merely" technical nor presumptively private, then they should be subject to more careful scrutiny with regard to the kind of citizen they produce. In particular, policy-makers cannot avoid engaging with the particular values that are encoded.

Configuration

Scholars in the umbrella field known as science and technology studies ("STS") have observed that although people design artifacts, artifacts also configure their users. Processes of configuration operate on several levels. First, designers of artifacts work with particular models of the user in mind, and those models have both intended and unintended effects.[3] Second, and more comprehensively, the artifacts that we use in our daily lives mediate our behavioral, perceptual, and heuristic relationships to the world around us. The particularities of their design make some actions seem easier and more natural, and other activities more difficult. These implicit behavioral templates, or affordances, encourage us to behave in certain ways rather than others.[4] Less remarked but often equally important, we tend to naturalize the operation of our artifacts—to experience the artifacts themselves as part of natural reality, and to perceive natural and social worlds through the lenses that they create.[5]

The processes of mediation and naturalization are old. In one sense, networked information technologies simply continue a process that has existed as long as humans have used tools. A mundane example of a predigital artifact that mediates our interaction with the world, familiar to many lawyers from the disability rights context, is the doorknob. A door with a doorknob is easier for some people to open than for others, and the difference profoundly shapes people's experience of the world around them. A world in which buildings and rooms are accessed via doors with doorknobs is trivially accessible for able-bodied adults and very nearly inaccessible for small children and those with certain disabilities. In the case of very small children, barriers to accessibility are usually a good thing; in the case of the disabled, however, barriers to accessibility have impeded equal participation in social and economic life.

Networked information technologies intensify the processes of mediation and naturalization. Consider now a more complicated example involving techniques of mapping and geolocation.[6] Twenty years ago, if one wanted to drive from one's own home to visit a friend in another town, one needed a map. Maps could (and still can) be purchased at bookstores and tourism offices or obtained from automobile clubs. To get from point A to point B, one studied the map, figured out the "lay of the land," and plotted a route. Internet mapping technologies changed that process; beginning about a decade ago, the Internet-savvy could use Mapquest or Google to plot their routes. When online route-plotting becomes the norm, it is possible to get from point A to point B without needing to figure out the route, or to take the "lay of the land," for oneself. One may, however, still have a general sense of the route to the extent that the printout shows a complete journey and provides some contextual details, such as major landmarks and whether travel will occur on highways or surface roads. Sometimes, online mapping services offer a choice of routes, which one can make using the contextual details that are available. Portable GPS technologies change the process of getting from point A to point B yet again. Now, one need not ever examine the proposed route in its entirety. One simply follows directions as they are given, one at a time. And one need not take the "lay of the land" at all.

As this example suggests, the mediation that networked information technologies perform is more complex in two interrelated ways. First, these technologies do not merely reshape the way we manipulate the world. They also represent the world, which creates the potential for more significant changes in the way that we make sense of it. They supply ready-to-hand representations that can free us from the need to create our own.

Second, networked information technologies do the work of mediation in a way that is more invisible to the ordinary user. In part this characteristic flows from the relative complexity of digital technologies and artifacts, but it also flows from prevailing norms of good design, which emphasize seamless, "user-friendly" interfaces that conceal the representational and heuristic work being done. Rules normalizing certain functions (for example, the plotting and display of travel routes, or the collection of information about users of a travel mapping service) can be distributed among technical intermediaries and embedded in the network, while users experience the effects of those rules as "just the way things are."

Consider now some other examples, directly related to processes of subject-formation and culture-formation, and by extension to the practice of citizenship:

Search: In the real world, access to information is mediated by a variety of physical and cultural factors, including geography and social convention. The technologies of online search and content delivery reshape existing patterns of accessibility. This is largely to the good; for those with access to the basic technical capability, networked information technologies and devices have dramatically increased access to information. Information networks do not simply negate barriers to access, however. Search engines like Google or Yahoo! rely on algorithms that read a variety of contextual clues about the relevance and appeal of particular items. Those algorithms in turn establish new geographies of access defined by a variety of factors, including semantic relatedness, popularity, and commercial interest.

In addition to providing and prioritizing different types of information, the online geographies of search and retrieval differ from physical geographies in other important ways. In particular, the rules that govern access can be more difficult to discern. Search engines configure us to expect every conceivable kind of information readily displayed at our fingertips. The rules that govern access seem to be neutral and natural, if we bother to interrogate them at all. Displays that segregate "real" results from sponsored ads add to the aura of neutral authority. In fact, the contents of search results are determined in part by users' own profiles and browsing histories; they are not neutral or natural in the least. More precise information about how search algorithms works generally is not available, however, because the search algorithms used by for-profit search companies are held as trade secrets.

The reconfiguration of search and accessibility reshapes the processes by which individuals and communities discover and make sense of information about the world. Early Internet scholars predicted that networked information technologies would produce an information environment characterized by greater openness and reduced censorship, but those predictions are not always borne out. Most obviously, some governments employ filtering technologies to restrict their citizens' access to information. Even in countries without a national firewall policy, however, coalescence around political affinity can produce a balkanizing effect. For example, recent examinations of the U.S. "Tea Party" movement suggest that "on the Internet" it is possible to exist in the echo chamber of one's own choosing, reading only sources that reinforce one's initial beliefs.[7] Other effects of reconfiguration are more general and subtle. By "personalizing" search and retrieval, the new semantic web technologies alter the nature of the serendipity that attends the activities of searching and browsing in ways that we have barely begun to understand.

Content Delivery: In the realm of content delivery, we have been accustomed to different kinds of access for different works—for example, bookstores for current or popular books and libraries for older or rarer books; record stores for the music we want to own and the radio for a more ephemeral listening experience; and so on. Online ventures blur the boundaries between distribution channels—between the library and the bookstore, between the record store and the radio, between the movie theater, the television, and the telephone. They also blur the boundaries between modes of access, including most notably copyright law's traditional distinction between the distribution of copies and one-time performance.

The processes of digital convergence have been described, and rightly so, as dramatically expanding the accessibility of knowledge goods. Again, however, networked information technologies do not simply increase access but also reconfigure it. For example, as online services become preferred routes for locating textual materials, the technologies for accessing information in book and periodical form are merging with the logics of commercialized search. In libraries, serendipitous encounters with knowledge traditionally have flowed from the physical process of browsing in the stacks or flipping through journal issues. For the most part, digital libraries have not yet effectively translated that capability to the digital realm. Digital cataloguing systems are cumbersome and hierarchically organized; they don't invite unstructured browsing the way real libraries do. Digital bookstores, in contrast, are innovators in search and recommendation, offering kinds of serendipity that users have learned to value enormously. But the serendipity that digital bookstores offer is different; it is based on commercially driven processes of personalization and prediction. The Google Book Search project takes that process to the next level, applying algorithm-driven personalization to full-text search.

Meanwhile, emerging technologies for delivery of digital media content increasingly incorporate protocols that restrict access to compliant (that is, authorized) devices. Designers of these technologies seek to reconfigure users' expectations about the content's manipulability—its amenability to being copied and remixed. In the case of digital music, users have resisted this reconfiguration because it radically altered capabilities they had come to expect. In the case of DVD movies and digital television standards, as to which users had fewer prior expectations, there was less resistance to overcome, and most users have more readily acquiesced to coded-in restrictions.[8] Conventions for delivery of text-based content ranging from news and opinion pieces to journal articles to books are still evolving.

Interaction: For many people, the modalities of social interaction have been dramatically altered by the emergence of "Web 2.0" technologies such as social networking services and content-sharing platforms. Just as physical architectures shape the terms of interaction in "real space," so the terms of online interaction are modulated by the features of digital architectures. If one subscribes to Facebook, for example, or uploads videos to YouTube, information is revealed or concealed, and connections made or refused, according to the options that each platform makes available.

Social networking platforms like Facebook configure their users to expect a relatively flat and large-grained universe of privacy possibilities. With very few tools for making fine-grained distinctions about the contextual appropriateness of particular disclosures, users who wish to take advantage of these platforms' connectivity must decide whether to disclose a large amount of information to most of their contacts or to disclose that information only to a select few. They also must learn to classify family, friends, and acquaintances according to a rigid and context-insensitive system that recognizes only a few categories.

The conventions instantiated by social networking platforms also alter the public discourse about secrecy and privacy. That result flows in part from social networking providers' complex and intertwined relationships with other commercial entities. Users' tastes and networks of contacts are valuable assets, and social networking platforms that seek to establish their own commercial viability can do so by selling access to their users. In addition, the large-grained and context-insensitive rules that mediate online disclosures create a climate in which embarrassing overdisclosures are inevitable and occur regularly, and in which users in turn become more highly attuned to disclosure-induced titillation and scandal.

In each of the areas described, networked information technologies and associated business models are configuring their users to expect particular capabilities and effects—to perceive a world mediated by the logics of search as unmediated reality, to experience the copying and remixing of cultural products as posing large legal risks, and to expect widespread disclosure and repeated scandal and spectacle in the domain of the personal. Those processes of configuration have potentially large consequences for the ways in which users gather information about the world, interact with their communities, form their own opinions of the good life, and define and pursue common goals.

In none of these cases are the changes just described the result of "technology" pure and simple. Technologies and artifacts do not have fixed, inevitable trajectories. In one of the foundational texts of STS, Langdon Winner posed the question whether particular classes of artifacts might nonetheless be said to have a definite politics.[9] He suggested that some technologies might be especially compatible with authoritarian or bureaucratic social forms—for example, nuclear warhead technology requires an authoritarian command structure. On that account, however, the technical and the social are even more tightly intertwined for "political" technologies than they are for "ordinary" ones. In either case, artifacts assume configurations that are determined by socially embedded values and priorities. Those configurations are an appropriate and important domain for law- and policy-making.

Configuration and Responsibility for Harm

To what extent should designers of networked digital artifacts bear legal responsibility for the ways that their design choices configure users? Legal scholars have long debated the extent to which legal responsibility for harms should be placed on third parties. In debates that range across topics from products liability to gun control to online copyright infringement, the arguments take on a predictable rhythm, in which theories about efficient prevention of harm clash with more libertarian takes on causation and responsibility. Defined by the liberty/efficiency binary, debates about responsibility tend to become zero-sum games, in which defendants are either fully responsible or fully immune from liability. That framing encourages judges and legal commentators to ignore more complicated questions about the institutional distribution of power—or, sometimes, to reason that a problem's complexity justifies declining to assign responsibility to any particular actor. The resulting inaction tends to reinforce the existing distribution of power rather than countering it.

In the arena of copyright policy, intermediary liability for online copyright infringement has been hotly contested. Scholars concerned with the preservation of individual liberties online have argued that placing responsibility for copyright infringement on providers of networked information technologies and communications services is unjust because those technologies and services are capable of a range of lawful uses. They argue that indirect liability doctrines are likely to result in the curtailment of long-cherished communicative freedoms, and to stifle productive innovation. On that reasoning, technology providers also should have no duty to modify their offerings to make third-party infringement more difficult.

Economic analysis, meanwhile, seems to point the other way; if liability for particular conduct is otherwise desirable, it should be allocated to the party or parties that can avoid harm for the lowest cost. On this reasoning, technology providers may legitimately be subjected to (re)design duties, even at some potential cost to user freedom. For now, at least, this view of the efficiency calculus appears to have gained the upper hand. Although indirect liability doctrines stop short of imposing specific design duties on providers of digital equipment and services, and so purport to balance freedom with obligation, the contours of liability are sufficiently uncertain to induce risk-averse firms to err on the side of caution.

Participants in these debates about responsibility for online copyright harms often seem tone-deaf to the broader effects of institutional and discursive power. The rules broadly distributing responsibility for infringement are cohering in predictable patterns that serve powerful and well-established interests. In particular, many emerging protocols for digital media devices and transmissions represent attempts to establish closed "regimes of authorization" that admit only compliant intermediaries.[10] Critically, such regimes encourage overpolicing by technology intermediaries in ways that disserve user interests in the freedom to engage in unstructured, open-ended interactions with cultural artifacts. This in turn undermines other important collective values that relate to cultural progress and to the quality of public discourse. Yet the extreme libertarian approach to technical design is equally untenable. On that view technology providers have no responsibility whatsoever for avoiding large harms either to legally sanctioned ownership interests or to the quality of public discourse more generally. And the polarization of copyright discourse proceeds at the expense of a productive middle ground that would involve defining the obligations of technology intermediaries more carefully.

In the privacy context, the polarities are reversed. Regulatory focus on the least cost avoider is either absent or sharply reduced, even though large processors of personal information are in the best position to prevent or minimize the risks of many privacy harms. Instead, most transfers of personal information in the United States are essentially unregulated. The Federal Trade Commission (FTC) has exercised oversight of privacy practices according to a notice-and-consent model, under which a firm processing personal information simply must disclose its privacy policy and honor the terms. In contexts where greater regulatory coordination is necessary, the FTC has shown a marked preference for so-called self-regulation by industry groups.

Civil libertarian arguments about privacy, meanwhile, do not uniformly support high privacy protection. Many such arguments privilege freedom of choice, including choices to surrender personal information in ways that may commodify the self. The FTC's regulatory stance likewise rests on the implicit judgment that individual transfers of personal information are generally consensual. Other libertarian arguments against privacy assert that state support for secrecy in any form undermines foundational principles of freedom of expression. Such arguments are not simply "constitutional" but rather ideological in character; they interpret core constitutional guarantees in a way that furthers a political economy of "communicative capitalism," in which flows of information are the engine of both politics and profit.[11]

Like the copyright debate about control, the privacy debate is tone-deaf to the inequalities that the commitment to openness creates. The notice-and-consent model, which facially appears to privilege liberty, concentrates all of the costs of controlling disclosures of personal information on the affected individuals. The resulting patterns of information flow disrupt the dialectical processes of boundary management that constitute privacy in practice and that situated subjects require in order to thrive.[12] The resulting "surveillant assemblages" do not simply render personal information accessible, but rather seek to render individual behaviors and preferences transparent and malleable by conforming them to preexisting frameworks.[13] It is true that no single commercial actor is responsible for "causing" online privacy harms; those harms are caused, instead, by the collective decision to do nothing (or very little) to stem the flow of information. At the same time, surveillant assemblages are vehicles for the exercise of power.

A few legal scholars have criticized the liberty/efficiency binary that dominates debates about responsibility and accountability precisely because it avoids the problem of ethical responsibility toward others. In a memorable essay about the deaths of children from gun violence, Mari Matsuda argued that legal rules about causation should be revised to reflect an ethic of care for the powerless.[14] Among other things, such a shift would entail distributing responsibility for harms suffered by disadvantaged persons broadly to powerful actors whose actions (or inactions) contributed to those harms. Matsuda's argument reminds us that facially neutral rules allocating responsibility can conceal a set of important background questions about distributive justice and ethical accountability.

Particularly in the high technology context, however, arguments about distributive justice do not squarely come to grips with the problem of configuration.[15] As we have seen, the current evolution of networked digital technologies is reconfiguring technology users to be passive consumers of media content and eager participants in the semantic web and the surveillance processes that feed it. That process raises questions not only about who should bear responsibility for harms but also about how that responsibility should be exercised. The choices involved are not the relatively simple choices that legal cases often present—for example, whether to reduce the probability of harm by x percent by adding a known safety measure that would increase a product's cost by y percent. They are more complex questions about how a design process with many moving parts should prioritize particular values. Relatedly, there are also questions of technological path-dependency to consider. Information-based products have complex life cycles, as do databases of consumer personal information. Thus, for example, assigning responsibility for contribution to invasions of privacy after the fact may do much less to advance the individual interest in privacy than we like to think.

Like the distributive justice argument, the problems of complexity and path-dependency force recognition of the fact that responsibility for information-based harms is not really binary at all. Participants in information markets already know this. For example, the gradual emergence of interlinked regimes of authorization in which many parties play roles in preventing the unauthorized spread of copyrighted content testifies to the fact that in the networked information age, responsibility for information flow is collective. As things now stand, however, the development of information law and policy for the networked information society does not seem to be proceeding in ways that comport with the ethic of care that Matsuda so powerfully articulates.

Perhaps, however, the problem is an institutional one. If courts cannot properly evaluate the distribution of responsibility, perhaps the problem is structural, and we might do better by placing that question in broader institutional perspective. Put differently, perhaps the distributive justice argument and the problem of configuration point to a type of responsibility that is more appropriately and effectively exercised elsewhere, in regulatory fora that might address the problem of configuration in a more systematic fashion.

Configuration and Governance

Another way to approach the question of legal responsibility for the ongoing configuration of networked individuals and communities is to consider more generally how society ought to structure accountability for the design of networked information technologies and artifacts. Among U.S. scholars of technology law and policy, those questions too have conventional answers. Many scholars who write about law and technology issues tend to think that the development of technical standards and the evolution of digital products and services are matters best regulated by the market rather than by government. Effective technology policy thus is a matter of respectful tinkering at the edge of essentially private processes.

It is tempting to read claims about the regulatory primacy of markets as restating a view of the public/private distinction that has long been discredited, and that regards certain types of activities as definitionally private.[16] Yet that formal view of the public/private distinction does not seem to be quite what contemporary legal scholars mean when they tout the superiority of market processes. Parsed more carefully, such claims reflect a more general shift in the tenor of scholarly conversations about the origins of effective "governance." 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. In these arguments, the incoherence of the public/private distinction is beside the point, and may even facilitate the movement of regulatory functions across the (problematized and possibly nonexistent) public/private divide.

The neorealist view of the process of governance held by many legal scholars of technology remains complicated in fundamental ways by liberal ideologies about the superiority of market processes. For example, a pillar of the neorealist faith in regulation-by-markets is a presumption about the market's relative speed and agility. But claims about the speed and agility of market processes tend not to account for technical and contractual path-dependencies. Collaboration in technology markets installs constellations of interests and commitments that span many generations of products and can be difficult to dislodge. This dynamic also calls into question the related presumption about the market's superiority as evaluator of technical merit; market participants tend to have their own precommitments and loyalties. Finally, government plays an important role in validating private technology processes, and not only because legal rules determine the "public" and "private" labels. Government actors are customers for technology products and services, and also are interested in advancing policy agendas of their own.

The technologies discussed above illustrate these complexities in operation. Although technical standards for protecting digital content and authorizing compliant implementations generally are developed via private standard-making processes, that process has been cumbersome and path-dependent. It also has entailed significant government involvement and support; for example, the FCC's rulemakings on the cable plug-and-play standard comprehensively involve the agency in standard-setting for access to digital broadcast content. So too with legal "standards": under the proposed Google Book Search settlement, the availability of books for online search would be regulated by privately negotiated and administered procedures, yet those procedures would bear the imprimatur of law and would bind a class of current and future claimants certified by the court. Notice-and-consent based regimes of privacy regulation, which represent an extreme devolution of regulatory authority upon private actors, generate path-dependencies that are inscribed in the design of information systems for storing, processing, and transferring user personal information. Still other examples discussed above are not thought to involve "regulation" at all; search engine algorithms, for example, tend to be understood as purely market creations, and on that understanding, the market also functions as ideological corrective to bias problems. That reasoning, however, is open to serious question for reasons that reveal the inextricable involvement of law. Search algorithms are objects of property, protected by trade secrecy laws from the sorts of disclosures that would enable markets to evaluate them. Notice-and-consent regimes of privacy protection similarly lack operational transparency, in large part because regulators have elected not to take a position on the granularity of disclosures regarding secondary market uses.

These examples raise serious questions about the philosophy of governance embodied in the four-modalities taxonomy—a philosophy whose libertarian core coexists uneasily with a willingness to abdicate effective control over decisions affecting an increasingly wide swath of sociotechnical activity. The word "governance" is supposed to denote a new methodological sophistication—a recognition that we have moved beyond government—but the four-modalities taxonomy does not incorporate considerations that political theorists consider critical, such as patterns of institutional interest and alignment. As some scholars have observed, contemporary models of "governance" bear a passing resemblance to Foucault's conception of "governmentality," in that they are premised on recognition of the pervasive diffusion of regulatory power throughout social institutions and discourses. At the same time, however, the enthusiastic embrace of privatized governance diverges from the Foucauldian approach to governmentality, which is concerned with mapping the distribution of power and subjecting it to critical scrutiny.[17] In operation, the four-modalities taxonomy of governance seeks simply to identify the most effective modalities of regulatory control, often in a relatively uncritical and technocratic fashion. For that reason, it is poorly suited to give regulators the critical purchase on the power imbalances that I identified in the previous section.

Determining the appropriate response to the de facto privatization of regulation by "code" is quite another matter. One might resort to the constitutional lawyer's time-tested strategy of asserting the essentially "public" nature of nominally private processes. Some scholars have made this argument in particular cases; for example, Danielle Citron argues that private-sector provision of electronic voting technologies should trigger due process guarantees.[18] At the same time, it is clear that federal agencies are not equipped to engage in technical standard-making for the multitude of products and services that the networked citizen now confronts. Reclassifying the private as public therefore seems unlikely to lead to a workable solution.

According to Jody Freeman, such reclassification also misses the most important lesson that the deconstruction of the public/private distinction teaches us: attempting to counter the drift toward privatized governance by reasserting a (problematized and possibly nonexistent) conception of the disinterested public good will not work.[19] Instead, she argues, we should embrace the public role in privatized governance by reconceptualizing governance through the lens of contract, as an extended process of public/private negotiation.

Freeman's proposal for reconfiguring the public-private regulatory relationship suggests some fruitful avenues to explore in the context of networked information technologies. In particular, it suggests that we ought to approach problems of regulatory design without precommitments to the superiority of "public" regulatory tools and processes. The traditional tools of government are neither the only nor the most useful tools for pursuing the implementation of public values.

Yet there is a mismatch of sorts between the model and the more accurate understanding of sociotechnical processes supplied by the STS literature. Freeman's model seems to presume a regulatory playing field in which the state of the technological art is held constant, and in which "technical" and "governance" issues are distinct. As we have seen, however, processes of contestation over the course of technological development go to the core of how the technologies are implemented. Government need not sit on the sidelines during that process, but instead can play a role in shaping governance processes in ways that distribute responsibility appropriately.

This argument derives unexpected theoretical support from the domain of economics. Economic theory identifies certain "public goods" that will not be produced absent state intervention, whether in the form of provision (national defense), subsidies (basic scientific research), or incentives (intellectual property). The emerging subdiscipline of public goods economics extends this core insight about potential underproduction to other classes of goods that generate large positive externalities, such as education, and argues that government ought to be responsible for ensuring sufficient production of those goods even if (and indeed precisely because) such provision entails "interference" in markets.[20] Like education, privacy and cultural play generate large positive spillovers for society; it is therefore incumbent upon society to ensure that they are produced in sufficient quantities.

The complexities of technological development suggest two important roles for public regulatory authorities. First, public regulators have an important role to play in designating particular values to serve as focal points for private standard-making. Such values might concern the scope of user "breathing room" to interact with digital media, or might establish broadly defined substantive privacy obligations around which private implementations might cohere. A template for this process is supplied by the "values in design" movement, whose practitioners articulate a design process organized around repeated definition, implementation, and iteration of critical and participatory values.[21]

Government also may demand accountability for the outcomes of private regulatory processes, and can tie that demand to particular metrics of success. For example, scholarship documenting and analyzing efforts to appropriate economic indicators as a technique for measuring the provision of human rights suggests that such "technologies of governmentality," although not without risks of their own, may help policy-makers to assess whether compliance with international obligations has been realized as a practical matter.[22] Critically, the metrics for accountability need not be the same as those used, for example, in measuring aggregate national welfare; they can be tailored to reflect distributions of income, education, access to communications and information, and cultural opportunity.

This general template for public/private cooperation leaves open the question of the particular values that the process should implement. That question brings us, finally, to the issue of citizenship. If networked information technologies mediate the practice of citizenship, the values articulated to serve as guideposts for the design process should connect to a larger vision of citizenship. This in turn suggests that law- and policy-makers have a more general, conceptual role to play in the design of "code."

Configuration and Citizenship

Theories of citizenship provide an alternative framework for structuring debates about accountability for the configuration of network users. To the extent that choices about the values encoded in technical architectures implicate the shaping of subjectivity and culture, they necessarily implicate the practice of citizenship by networked, situated subjects. In general, the leading theoretical approaches to citizenship are highly attuned to questions about how the structure of information markets affects the practice of citizenship. However, liberal and neoliberal theories of citizenship tend to be relatively insensitive to questions of sociotechnical configuration. Theories of sociotechnical configuration, for their part, tend to be relatively insensitive to the question of citizenship and how it is to be exercised. To some extent the divide traces back to first principles; theories of citizenship often (though not always) have close ties to liberal political theory, while theories of sociotechnical configuration tend to be aligned with critical theory. As the dependence of individuals, communities, markets, and governments on networked information technologies intensifies, the need for some rapprochement between the two literatures and their respective concerns has become more pressing. Emerging critical-pragmatist theories of technology, and of citizenship, offer a way forward for thinking about the relation between technology and citizenship in the networked information age.

The liberty/efficiency binary that dominates debates about responsibility for copyright infringement, and that appears to dictate a systemic lack of responsibility for technology-driven harms to privacy, is broadly consonant with a neoliberal philosophy of government in which citizens are defined through their autonomous choices as consumers of goods, services, and information. Within neoliberal theories of political economy, citizens exercise their voice principally as consumers, by voting for or against particular candidates, by purchasing or declining to purchase access to particular goods and services, and by using or refraining from use of particular technologies.

The neoliberal vision of government and citizenship also animates debates about the possible regulatory oversight of technical design processes. What Jodi Short describes as "the paranoid style in regulatory reform" is very much in evidence in the legal and policy literature about code and law.[23] The particular understanding of the relationship between public and private that animates regulatory debates about new digital technologies is one in which scholars and policy advocates are deeply concerned about the risks of state coercion and state bumbling, and relatively insensitive to other worries.

Liberal theories of citizenship recognize a more robust role for the citizen but differ on how the condition of active, informed citizenship is to be achieved. While some theorists presume a baseline level of autonomy and a correspondingly active agency, others argue that those presumptions are unrealistic in light of existing patterns of inequality. Matsuda's concern for the distributive implications of causation rules resonates with a differentialist model of citizenship within which the least powerful require the law's special protection. Within Matsuda's vision, law fulfills its core mission only when it articulates and puts into practice an ethic of care for the least fortunate.

The gap between neoliberal and liberal theories of citizenship is well explored, and I will not belabor it here. This chapter is concerned with a different sort of gap: even differentialist defenses of liberal citizenship leave unaddressed important questions about the sociotechnical dimension of citizenship. In particular, two kinds of questions remain to be answered: what capabilities are necessary for the practice of citizenship in an increasingly networked information society, and whether the practice of citizenship in the emerging networked information society ought to be linked to any particular substantive vision of what citizenship entails.

The theory of capabilities for human flourishing supplies the beginnings of an answer to the first question. One might characterize capabilities theory as concerned with establishing the conditions for the practice of citizenship. Human flourishing encompasses a range of needs beginning with the most general and basic conditions for physical survival and well-being, but also including higher-order needs. As developed by Martha Nussbaum, Amartya Sen, and others, the theory points to the capabilities necessary for individuals and communities to form and pursue a vision of the good life.[24] This necessarily implicates the practice of citizenship, and the connection is often explicit. Nussbaum's taxonomy of essential capabilities includes the ability to exercise effective political control over one's environment, and also touches on citizenship at various other points.[25]

As I have argued, however, translating the relatively abstract vision of capabilities for human flourishing into the networked information environment requires greater attention to the importance of both information and materiality. The literature generated by the "access to knowledge" (A2K) movement addresses some of these issues, pointing to the importance of access to information and networked information technologies in the emerging networked information society.[26] Yet both Nussbaum's articulation of the capabilities approach and the version of the capabilities approach developed in the A2K literature are weak precisely on the issue of configuration. Nussbaum's taxonomy of essential capabilities treats the material environment as either the subject of property or as inert matter. The approach developed in the A2K literature suffers from inattention to the material realities of everyday experience; this leads scholars affiliated with the A2K movement to overvalue "openness" and to undervalue privacy.

A regime of information policy designed to promote human flourishing in the networked information society can address concerns about material enablement in two general ways.[27] First, technical architectures should be subject to a requirement of operational transparency. To exercise meaningful control over the development of critical subjectivity, the networked self needs adequate information about how the network and its constituent artifacts and protocols work and access to the processes in which network standards are designed. Second, information law and policy should seek to foster semantic discontinuity within technical and information landscapes. The emerging networked information society is characterized by increasingly seamless and granular regulation of information access and use, and by increasingly precise efforts to monitor and predict individual behavior with comparable seamlessness and granularity. This diminishes the ability of individual users and communities to encounter and interact with flows of culture, and to pursue contextually specific practices of self-definition, in patterns that form and re-form more organically. Information law and policy should foster interruptions in the legal, market, and technical frameworks that define information rights and obligations, to preserve room for such practices and patterns.

The second question, about the need for a substantive vision of citizenship to animate regulatory reform, directs our attention to the ways in which emerging sociotechnical configurations enable or disable not only particular capabilities, but also particular understandings of what “citizenship” entails. One possibility is that the design of “code” might prize a more explicitly nationalist vision in which “imagined communities” articulate themselves in part through technical architectures and rules.[28] Internet technology and policy elites purport to reject such a vision, arguing that the Internet hastens convergence around universal values of openness. The values of most Internet elites are not neutral, however; they are Western and often American values. As Laura DeNardis shows, this demographic bias has given Internet standards proceedings a pronounced American slant.[29] As a practical reality, moreover, information policy is not made only in global standards processes, and information policy debates are peppered with national differences. Consider, for example, debates about the sale of Nazi memorabilia on eBay, which have raised questions about whose vision of free speech online ought to dominate. As another example, the European stance on information privacy is much different than that of the United States.

In Nussbaum’s articulation, the theory of capabilities for human flourishing is explicitly linked to a postnationalist, or cosmopolitan, vision of how citizenship is to be achieved.[30] Although it rejects instrumental assertions of national difference, the cosmopolitan vision of citizenship also cannot avoid being culturally determined; it is a Western vision that traces its origin to particular liberal values. Yet it strives for a relative universality that rejects social contractarian justifications for nationalist policies. Whether that view translates into particular prescriptions for the design of technology beyond a commitment to open source and open access is a question that A2K theorists generally have not considered.

How are we to choose between these approaches? It is worth noting, first, that arguments for nation-specific technology policy are not always or inevitably linked to nationalist theories of citizenship. In the realm of privacy, for example, European regulators believe that their approach better serves universal requirements of human dignity, and would prefer to see it adopted everywhere. To the extent that technology policy debates are rooted in more fundamental disagreements about nationalism versus cosmopolitanism (as seems to be the case, for example, in the controversy over Chinese

Internet policy), there does not seem to be a principled way to decide. If we attend instead to the problem of sociotechnical configuration and to the linked problematic of subject-formation, moreover, the question of nationalism versus cosmopolitanism seems imprecisely focused. National and cultural differences in technology policy are to some extent inevitable. It becomes relatively more important to pay attention to the processes by which power relations are encoded in technologies and artifacts. This is something that liberal theories of citizenship do not generally do.

Theories of sociotechnical configuration, in contrast, typically regard the foundational commitments of liberal political theory with suspicion, and instead manifest allegiance to some version of critical or radical political theory. Although there are important differences among theorists of technology, their primary concern is with the hidden exercise of power.[31] Yet with hidden power everywhere around us, the way forward for a theory of citizenship can be difficult to discern.

Contemporary work at the intersection between pragmatist theories of citizenship and critical theory offers a promising approach to integrating theories of sociotechnical configuration with theories of citizenship. The critical-pragmatist theories recently outlined by several scholars, including Larry Hickman and Alison Kadlec, supply a normative grounding for an approach to both citizenship and sociotechnical configuration that is both rigorous and antifoundationalist.[32] Both scholars draw on the writings of John Dewey, and argue that Dewey's political theory is neither normatively anemic (as liberal theorists and communitarian theorists have asserted) nor indifferent to power (as critical theorists would have it), but rather supplies the foundation for an ethical approach to both politics and technology in an age of uncertainty. According to Hickman and Kadlec, the essence of democratic citizenship is not a particular position of normative privilege, and indeed no such position is epistemologically possible. Instead, the essence of democratic citizenship is a critical stance toward existing alignments of power and an openness toward revising one's understanding of reality through experience and change. This stance in turn dictates a critical interventionist approach to technical architectures.

A critical-pragmatist approach to the practice of citizenship in the emerging networked information society sheds some useful, albeit preliminary, light on the question about nationalism versus universalism. What is troubling is not nationalist or universalist technology policy per se, but invisible processes of configuration deployed to buttress particular nationalist or universalist policies. Technical and sociotechnical opacity obscure the connections between configuration and the practice of citizenship, disabling both citizens and nations from self-determination. In an age in which human interactions are comprehensively mediated by networked information technologies, a universalist stance toward ensuring that technical architectures are transparent and open to revision is essential.

In particular, a critical-pragmatist approach to the practice of citizenship in the emerging networked information society suggests two kinds of intervention in processes of sociotechnical configuration. First, it dictates careful attention to the design of ostensibly "technical" governance processes. Such processes should be designed in ways that make connections between the "technical" and the "political" more explicit. This process of gap-bridging requires more than merely translation if it is to be adequate. The obligation to promote human flourishing, and to create the conditions for the effective and active practice of citizenship, cannot be satisfied if information about technical governance processes flows only one way. The practice of citizenship requires both adequate representation in sociotechnical processes and input into the articulation of values to be instantiated in design.

Second, a critical-pragmatist approach to the practice of citizenship suggests the development of design principles intended to remind people that their actions and interactions are comprehensively mediated by their artifacts, and that alternative possibilities for both action and design exist. For example, if the current evolution of the blogosphere contributes to an echo chamber effect, a critical-pragmatist approach to governance would give consideration to how practical encounter with a diversity of viewpoints is to be achieved.[33] For example, one might imagine a set of mandates designed to achieve an "architecture of discomfort" that would force people to encounter opposite points of view, or softer mandates designed to signal their availability and invite exploration. Other regulatory interventions might seek to encourage the design of social networking platforms in ways that remind users of the choices to be made, and that incorporate user feedback about the need for contextual separation. Interventions like these would serve as reminders that technical design is properly the subject of politics, and an important domain of ethical and moral choice.

Conclusion

Networked information technologies and communications devices constitute a new regulatory landscape in which attention must be paid not simply to questions about what conduct is permitted or prohibited, but more generally and systemically to questions about the affordances that networked artifacts manifest and quality of the subjectivity that they produce. Those questions are neither technical nor of purely private concern, and to treat them that way is a mistake. Networked information technologies and communications devices already distribute responsibility for the configuration of networked citizens more broadly across a variety of network intermediaries. Regimes of sociotechnical configuration are a legitimate and urgent subject of public concern.

The unique combination of invisibility and restriction that characterizes many emerging networked information and communications technologies has powerful implications for human flourishing in the networked information society. There is no countervailing set of rules broadly distributing responsibility for promoting human flourishing and enabling the practice of citizenship, but there should be. Articulating such rules requires dissolving the liberty/efficiency binary, rejecting the presumptive privatization of "governance," and parsing more carefully the ways in which regulatory processes might allocate responsibility among a variety of actors. In particular, recognizing and responding to the problem of sociotechnical configuration requires a model of governance premised on the reassertion of “public” values and the harnessing of resources and actors on both sides of the public-private divide in pursuit of important collective goals. A critical-pragmatist approach to the exercise of citizenship in the networked information society should seek to foster widespread awareness of the problem of configuration and to instill appreciation of the importance of continual, critical revision in the domain of the sociotechnical.

Notes

Thanks to Lawrence Douglas, Austin Sarat, and Martha Merrill Umphrey for their helpful comments, and to June Casey and the staff of the Langdell Law Library at the Harvard Law School for research assistance.

1. Lawrence Lessig, *Code and Other Laws of Cyberspace* (New York: Basic Books, 1998).

2. Julie E. Cohen, *Configuring the Networked Self: Law, Code, and the Play of Everyday Practice* (New Haven: Yale University Press, forthcoming January 2012).

3. See, for example, Steve Woolgar, “Configuring the User,” in *A Sociology of Monsters: Essays on Power, Technology and Domination*, ed. John Law (New York: Routledge, 1991), 57–99.

4. See Brian Pfaffenberger, “Social Anthropology of Technology,” 21(1) *Annual Review of Anthropology* (1992), 491–516.

5. See Peter-Paul Verbeek, *What Things Do: Philosophical Reflections on Technology, Agency, and Design*, trans. Robert P. Crease (University Park, PA: Pennsylvania State University Press, 2005).

6. This example is adapted from Cohen, *Configuring the Networked Self*, ch. 2.

7. See Tim Mak, “Inside the Tea Party Echo Chamber,” *Frum Forum*, March 16, 2010, http://www.frumforum.com/frum-forum-surveys-the-tea-partiers; see also Kathleen Hall Jamieson and Joseph N. Cappella, *Echo Chamber: Rush Limbaugh and the Conservative Media Establishment* (New York: Oxford University Press, 2008); and William Saletan, “Bubble Think: How to Escape a Partisan Echo Chamber,” *Slate*, May 3, 2010.

8. Tarleton Gillespie, *Wired Shut: Copyright and the Shape of Digital Culture* (Cambridge, MA: MIT Press, 2007).

9. Langdon Winner, “Do Artifacts Have Politics?” in *The Whale and the Reactor: A Search for Limits in an Age of High Technology*, ed. Winner (Chicago: University of Chicago Press, 1986).

10. On regimes of authorization, see Cohen, *Configuring the Networked Self*, ch. 8.

11. Jodi Dean, *Publicity’s Secret: How Technoculture Capitalizes on Democracy* (Ithaca, NY: Cornell University Press, 2002).

12. Irving Altman, *The Environment and Social Behavior: Privacy, Personal Space, Territory, Crowding* (Monterey, CA: Brooks/Cole Publishing, 1975).

13. See Kevin D. Haggerty and Richard V. Ericson, “The Surveillant Assemblage,” 51(4) *British Journal of Sociology* (2000), 605–22.

14. Mari Matsuda, “On Causation,” 100 *Columbia Law Review* (2000), 2195–2220.

15. Debates about causation and responsibility in the privacy context articulate the problem of configuration, if at all, in a way that is a function of privacy law’s concern with expectations. The problem

with privacy claims, we are told, is that expectations can change—as though the patterns of change were themselves natural and organic rather than a function of artifactual design.

16. See, for example, Duncan Kennedy, "The Stages of the Decline of the Public/Private Distinction," 130(6) *University of Pennsylvania Law Review* (June 1982), 1349–57; and Karl Klare, "The Public/Private Distinction in Labor Law," 130(6) *University of Pennsylvania Law Review* (June 1982), 1358–1422.

17. Michel Foucault, "Governmentality," in *The Foucault Effect: Studies in Governmentality*, ed. Graham Burtchaell, Colin Gordon, and Peter Miller, rev. trans. Colin Gordon (Chicago: University of Chicago Press, 1991), 87–104. For a survey of the contemporary literature on governance, see Scott Burris, Michael Kempa, and Clifford Shearing, "Changes in Governance: A Cross-Disciplinary Review of Current Scholarship," 41 *Akron Law Review* (2008), 1–66.

18. Danielle Keats Citron, "Technological Due Process," 85(6) *Washington University Law Review* (2008), 1249–1313.

19. Jody Freeman, "The Private Role in Public Governance," 74(3) *New York University Law Review* (2000), 543–675.

20. For a helpful summary, see Margaret Chon, "Intellectual Property and the Development Divide," 27(6) *Cardozo Law Review* (April 2006), 2821–2912.

21. See, for example, Batya Friedman, ed., *Human Values and the Design of Computer Technology* (New York: Cambridge University Press, 1997).

22. AnnJanette Rosga and Margaret L. Satterthwaite, "The Trust in Indicators: Measuring Human Rights," 27(2) *Berkeley Journal of International Law* (2009), 253–315.

23. Jodi L. Short, "The Paranoid Style in Regulatory Reform," working paper (2010).

24. See, for example, Martha C. Nussbaum, "Aristotelian Social Democracy," in *Liberalism and the Good*, ed. R. Bruce Douglass et al. (New York: Routledge, 1990), 203–52; Nussbaum, *Frontiers of Justice: Disability, Nationality, Species Membership* (Cambridge, MA: Belknap, 2006); Amartya Sen, *Development as Freedom* (New York: Anchor, 1999); Sen, *Inequality Reexamined* (Cambridge, MA: Harvard University Press, 1992); and Sen, "Elements of a Theory of Human Rights," 32(4) *Philosophy and Public Affairs* (October 2004), 315–26.

25. Nussbaum, *Frontiers of Justice*, 76–78.

26. For a representative taxonomy, see Lea Bishop Shaver, "Defining and Measuring A2K: A Blueprint for an Index of Access to Knowledge," 4(2) *I/S: A Journal of Law and Policy for the Information Society* (Summer 2008), 235–69.

27. For a detailed discussion, see Cohen, *Configuring the Networked Self*, ch. 9.

28. Benedict Anderson, *Imagined Communities* (New York: Verso, rev. ed. 1991).

29. Laura DeNardis, *Protocol Politics: The Globalization of Internet Governance* (Cambridge, MA: MIT Press, 2009).

30. Nussbaum, *Frontiers of Justice*, 273–324.

31. See, for example, John Law, ed., *A Sociology of Monsters: Essays on Power, Technology, and Domination* (New York: Routledge, 1991).

32. Larry Hickman, *Philosophical Tools for Technological Culture: Putting Pragmatism to Work* (Bloomington: Indiana University Press, 2001); Alison Kadlec, *Dewey's Critical Pragmatism* (Lanham, MD: Lexington Books, 2007).

33. See Jutta Treviranus and Stephen Hoekema, "The Value of the Unpopular: Counteracting the Popularity Echo-Chamber on the Web," IEEE TIC-STH 2009, 603–08.