Philos. Technol. (2018) 31:213–233
DOI 10.1007/s13347-017-0258-2

RESEARCH ARTICLE

The Biopolitical Public Domain: the Legal Construction of the Surveillance Economy

Julie E. Cohen [1]

Received: 30 September 2016 / Accepted: 15 March 2017 / Published online: 28 March 2017

Abstract Within the political economy of informational capitalism, commercial surveillance practices are tools for resource extraction. That process requires an enabling legal construct, which this essay identifies and explores. Contemporary practices of personal information processing constitute a new type of public domain—a repository of raw materials that are there for the taking and that are framed as inputs to particular types of productive activity. As a legal construct, the biopolitical public domain shapes practices of appropriation and use of personal information in two complementary and interrelated ways. First, it constitutes personal information as available and potentially valuable: as a pool of materials that may be freely appropriated as inputs to economic production. That framing supports the reorganization of sociotechnical activity in ways directed toward extraction and appropriation. Second, the biopolitical public domain constitutes the personal information harvested within networked information environments as raw. That framing creates the backdrop for culturally situated techniques of knowledge production and for the logic that designates those techniques as sites of legal privilege.

Keywords Surveillance · Informational capitalism · Biopolitics · Public domain · Data · Big data · Personal information · Postcolonialism

1 Introduction

The information extracted from individuals plays an increasingly important role as raw material in the political economy of informational capitalism. Personal information processing has become the newest form of bioprospecting, as entities of all sizes

Julie E. Cohen is Mark Claster Mamolen Professor of Law & Technology, Georgetown Law.

✉ Julie E. Cohen
jec@law.georgetown.edu

[1] Georgetown University Law Center, Washington, DC, USA

compete to discover new patterns and extract their marketplace value. Understood as processes of resource extraction, the activities of collecting and processing personal information require an enabling legal construct. The essay identifies that construct—one foreign to privacy and data protection law but commonplace within intellectual property law—and traces its effects.

Contemporary practices of personal information processing constitute a new type of public domain, which I will call the *biopolitical public domain*: a repository of raw materials that are there for the taking and that are framed as inputs to particular types of productive activity. The raw materials consist of information identifying or relating to people, and the public domain made up of those materials is biopolitical—rather than, say, personal or informational—because the productive activities that it frames as desirable are activities that involve the description, processing, and management of populations, with consequences that are productive, distributive, and epistemological.

The construct of a public domain both designates particular types of resources as available and suggests particular ways of putting them to work (Litman 1990). It thereby legitimates the resulting patterns of appropriation and obscures the distributive politics in which they are embedded (Chander and Sunder 2004). The biopolitical public domain conforms to these patterns, constituting the field for appropriation and use of personal information in two complementary and interrelated ways. First, it constitutes personal information as *available and potentially valuable*: as a pool of materials that may be freely appropriated as inputs to economic production. That framing supports the reorganization of sociotechnical activity in ways directed toward extraction and appropriation. Second, the biopolitical public domain constitutes the personal information harvested within networked information environments as *raw*. That framing creates the backdrop for culturally situated techniques of knowledge production and for the logic that designates those techniques as sites of legal privilege.

The construct of the biopolitical public domain is foreign to privacy and data protection law, but its effects are not. Materials constituted as part of the biopolitical public domain are effectively designated as always-already public in ways that foreclose real discussion of that designation. It therefore helps to explain the curious disconnect between privacy law and theory, which presume the existence of individual claim rights to control flows of personal information, and prevailing practices within the surveillance economy, which more often than not seem to brush such claims aside.

2 Imagining Public Domains

The process of constructing a public domain begins with an act of imagination that doubles as an assertion of power. An identifiable subject matter—a part of the natural world or an artifact of human activity—is reconceived as a resource that is unowned but potentially appropriable, either as an asset in itself or as an input into profit-making activity. The biopolitical public domain is a construct tailored to the political economy of informational capitalism. It constitutes the field of opportunity for a particular set of information-based extractive endeavors.

To the contemporary mind, the idea of a public domain is most closely associated with regimes of intellectual property, but it has older roots in the era of global exploration and conquest. For the early explorers and the European sovereigns who financed their voyages,

the act of naming and staking claim to hitherto undiscovered lands marked those lands as ownable resources and their contents as available for harvesting or capture.[1] Later, for the fledgling government of the USA, the idea of a public domain available to be claimed by the state and then parceled out to deserving claimants gave tangible purchase to narratives of inevitable and productive westward expansion and manifest destiny (Feller 1984; Gates 1996). The copyright and patent regimes that emerged during the nineteenth century in Europe and the USA depend centrally on the idea of the intellectual public domain as a repository of raw materials upon which future authors and inventors can build. One may not lay exclusive claim to inputs from the intellectual public domain, but resources in the public domain may be freely appropriated as the basis for profitable activity.

In both real property law and intellectual property law, the idea of a public domain thus both emphasizes and assumes two conditions. The first is abundance. As political philosopher John Locke (1947, p. 145) put it in 1690, "in the beginning all the World was America." That framing is revelatory; it depends for its intelligibility on an understanding of America as *terra nullius* unowned and available for occupation. Formulated at a historical moment when the world still seemed limitless enough to satisfy all conceivable sources of demand, it expresses a heady sense of infinite possibility. In contemporary intellectual property debates about the exploitation of intangibles, which are nonrivalrous, the constraints of scarcity have seemed even more remote. Ideas, facts, and scientific principles are understood as paradigmatic examples of renewable resources; it is thought inconceivable that we could ever run out.

The second condition that the idea of a public domain presumes is the absence of prior claims to the resource in question. America in 1690 was not *terra nullius* to its native inhabitants, but their traditions of occupancy and use were not understood as ownership claims by European explorers and colonists. Similarly, intellectual property regimes traditionally have taken a dismissive stance toward those claiming interests in folk art and traditional knowledge. In the modern era, that stance has encouraged the intellectual equivalent of a land rush by the mass culture industries, pharmaceutical companies, and other information businesses. The resulting patterns of exploitation have predictable geographies. Scholars who study the global intellectual property system have mapped a distinctive pattern of information flow, in which resources extracted from the global South flow north twice: once as indigenous resources extracted and appropriated by intellectual property industries headquartered in the global North and a second time as payments exacted for products based on those resources (Chander and Sunder 2004).

The idea of a public domain thus reflects an implicit distributive politics, with important, real-world consequences for the distribution of both political power and economic wealth. Put differently, a public domain is a construct through which political-economic power is exercised. The biopolitical public domain conforms to that pattern. More specifically, it is a construct that enables both the marshaling of informational resources and the exercise of biopower over subject populations within the political economy of informational capitalism.

Contemporary descriptions of the commercial future of personal data processing contain numerous examples of framing in terms of abundance and infinite possibility.

[1] Within the U.S. legal system, the definitive treatment of these questions is Johnson v. M'Intosh, 21 U.S. 543 (1823).

In marketing brochures and prospectus statements, information businesses of all sorts describe in glowing terms the ways that processing of personal information will open new and profitable lines of exploration. Data broker Intelius boasts: "Our robust technology enables us to gather billions of public records annually from a multitude of government and professional entities and assign them to more than 225 million unique people." TowerData (formerly Rapleaf) promises "data on 80% of email or postal addresses," and CoreLogic touts its access to "more than 3.5 billion records" and its focus on "turning mountains of data into valuable insights"[2] These optimistic pronouncements, which herald the dawn of a new age of data science, constitute the ever-expanding universe of personal information as a *terra nullius* for enterprising data developers, an unexplored frontier to be staked out, mapped, and colonized.

Those descriptions also reflect a familiar distributive politics. Commercial surveillance practices deploy powerful new data processing techniques to map and monetize subject populations, and those who undertake that project speak and behave in ways that express unquestioned assumptions about their rights to appropriate and exploit that which is freely available. According to Experian, "Marketing data differs in important ways from consumer credit data. Experian's marketing data is drawn primarily from public records and other publicly available sources."[3] Google Chief Economist Hal Varian (2014) reports: "Google runs about 10,000 experiments a year in search and ads. There are about 1,000 running at any one time, and when you access Google you are in dozens of experiments." In these and similar statements, all the world is America again, and doubly so: The information resources extracted from populations worldwide flow into the databanks of the new information capitalists, who then use those resources to devise new profit-making strategies. And both in the USA and worldwide, U.S. information companies are in the forefront of the race to harvest the resources of the biopolitical public domain and make them productive.

As we will see in the balance of this paper, the political-economic power of the biopolitical public domain construct unfolds on two levels. First and generically, it facilitates the ongoing process of economic transformation to an informational economy. Just as the transition from agrarianism to industrialism appeared to demand the unbridled commodification of labor, land, and money (Polanyi 1957), so the transition from industrialism to informationalism (Castells 1996) now appears to require the commodification of other important resources. The simplicity of that syllogism, of course, is deceptive and points toward the second and more fundamental way in which the biopolitical public domain facilitates the exercise of power: It represents an especially precise strategy for the exercise of biopower (Foucault 1978, 2007) over subject populations. It thereby exemplifies several themes that have surfaced in debates about the relevance of biopower as a theoretical framework for analyzing the contemporary political and economic landscape. The extractive strategies that it enables operate via control of flows of networked information (Deleuze 1995), lending

[2] Intelius, "About," http://corp.intelius.com/; TowerData, "Enhance Your Email List with Email Intelligence," http://www.towerdata.com/email-intelligence/overview; CoreLogic, "Data: Breadth and Depth," http://www.corelogic.com/about-us/our-company.aspx#container-Data.

[3] Hearing before the Senate Committee on Commerce, Science, and Transportation, "What Information Do Data Brokers Have on Consumers, and How Do They Use It?", 113th Cong., 1st Sess., December 18, 2013 (statement of Tony Hadley, Senior Vice President of Government Affairs and Public Policy, Experian).

additional force to the argument equating biopower with "the management of fluctuating processes in an open field" (Nail 2016, p. 259). In constituting populations as collections of data doubles, those extractive strategies continue a longer historical pattern within which evolving forms of capitalism appear to elicit and naturalize specific techniques for population management (cf. Gros 2016; see also Zuboff 2015).[4] The construct of the biopolitical public domain therefore also represents disciplinary power made light and nimble for the age of neoliberal individualism. As it pursues the project of surplus extraction, power over flows of personal information modulates participation in the evolving global marketplace for goods and services and simultaneously enlists populations in their own construction as depoliticized subjects defined by their consumptive choices (cf. May and McWhorter 2016).

3 Logics of Abundance and Extraction

Imagining the universe of personal data as a commons is only the beginning, however. For the idea of a public domain to fulfill its imagined destiny as a site of productive labor, it must be linked to more concrete logics of extraction and appropriation. By that standard, the biopolitical public domain is a construct of extraordinary power. As this section describes, the idea of a public domain of personal data has catalyzed far-reaching reorganizations of sociotechnical activity to facilitate harvesting personal data "in the wild" and to mark such data, once collected, as owned.

3.1 Digital Breadcrumbs

The discovery of the biopolitical public domain dates to 1994, when a researcher at the Netscape Corporation named Lou Montulli developed a protocol for identifying visitors to web sites. The protocol involved insertion of a small piece of code—which Montulli named a "cookie"—into the user's browser. This enabled so-called stateful interactions, such as transactions involving use of a virtual shopping cart. Implemented in "persistent" form, it also could enable reidentification of those users when they returned to the site later on (Kristol 2001). Netscape and other technology companies quickly recognized that cookies could play a key role in transforming the Internet into an infrastructure for commercial communications. Netscape implemented the technology in its Navigator browser and filed a U.S. patent application in Montulli's name. In 1995, recognizing the promise of cookie technology as a standard for state management and seeking to avert technical inconsistency in implementation, the Internet Engineering Task Force (IETF) formed a working group to develop a formal specification (ibid.).

Initial implementations of cookie protocols by both Netscape and Microsoft were nontransparent to users, but the technology was open in an entirely different sense: it dramatically expanded the opportunity to participate in commercial surveillance

[4] Gros's later periodization (from industrial to managerial and then financial capitalism) ignores the underlying transformative importance of the sociotechnical shift to informationalism as a mode of development; Zuboff's important formulation (surveillance capitalism) nonetheless ignores certain other important dimensions of informational capitalism, particularly those that revolve around intangible intellectual property entitlements.

activity. The customer databases within which processes of customer profiling originated were walled gardens, developed and maintained by consumer credit issuers for their own private purposes (Gandy 1993; Manning 2000). Customer profiles could be sold, but collecting new data required a preexisting relationship with the customer. Cookies changed all of that. Anyone with a server connection to the Internet could become a data collector, and cookies also could be served and collected by third parties providing hosting, payment, or marketing services.

The significance of this restructuring of surveillance capacity is evident from the nature of the marketplace response. Although the commercial Internet was in its infancy, marketers and advertisers rushed to adopt and improve upon the new technology. Increasing public and regulatory scrutiny of cookies did nothing to dampen their enthusiasm. Even as Netscape and other browser developers began to build greater transparency and user control into subsequent iterations of their browsers, the commercial web resisted both efforts. Willingness to accept at least some kinds of cookies became an increasingly necessary precondition for transacting online and participating in online communities. In addition, marketers and technologists in their employ developed a set of less-visible tracking techniques, known variously as "clear GIFs" or "web bugs,"[5] for surreptitiously collecting information about Internet users' behavior.

Similarly, although the IETF working group had identified the privacy issues raised by cookies very early on, efforts to write a uniform level of heightened user control into the standard met with pushback. Technology companies preferred a more minimal standard that would afford greater flexibility in implementation, and members of the rapidly growing online advertising industry sought to preserve the possibility of a promising new business model. The IETF standards process had not previously experienced intensive public policy scrutiny, and working group members were unused to evaluating and responding to political and policy objections. The group had difficulty bringing the standards process to closure, and the delay allowed the more minimal standard to become entrenched within industry practice (Kristol 2001).

In the USA, efforts to enact legislation restricting the use of so-called spyware failed repeatedly. Merchants and communications providers that deployed cookies for what they saw as legitimate purposes balked at definitional language extending labels like "spyware" and "cybertrespass" to their own activities. Both the venerable Direct Marketing Association and the newly formed Network Advertising Initiative lobbied strongly on behalf of the advertising industry against language that would sweep in too many uses of the new techniques. Other entities, including Microsoft Corporation, urged Congress to move cautiously to avoid foreclosing innovative market responses.[6] In three successive sessions of Congress, bills that would have provided a framework to constrain the use of automated tagging and tracking protocols died in committee.

[5] Richard M. Smith, "The Web Bug FAQ," Nov. 11, 1999, https://w2.eff.org/Privacy/Marketing/web_bug.html.

[6] See, for example, Hearing before the Senate Committee on Commerce, Science & Transportation, "Spyware," 109th Cong., 1st Sess., May 11, 2005 (statement of Trevor Hughes, Executive Director, Network Advertising Initiative); Hearing before the House Committee on Energy and Commerce, "Combating Spyware: H.R. 29, the SPY Act," H.R. No. 109–10, 109th Cong., 1st Sess., January 26, 2005, pp. 17–14 (statement of Ira Rubinstein, Associate General Counsel, Microsoft Corporation).

In the absence of a regulatory framework specifically tailored to the problems of surreptitious tracking and "behavioral advertising," the Federal Trade Commission asserted its general authority to regulate unfair and deceptive practices in commerce. As a practical matter, this meant that notice and consent became the dominant regulatory framework for evaluating online businesses' use of cookies, and the "privacy policy"—a lengthy, turgid document disclosing general categories of information about an online entity's collection and processing of personal information—became the de facto vehicle for ensuring compliance. The FTC has vigorously policed the content of privacy policies and the timing of privacy policy changes (Solove and Hartzog 2014), but experience and research have shown that consumer choice, easily manipulated, is a relatively ineffective vehicle for constraining commercial data collection and processing (Acquisti et al. 2015; Willis, 2013, 2015).

At the same time, the quest to track Internet users by less transparent means continued, pushing deeply into the logical and hardware layers of consumers' devices. Advertising technology companies began developing techniques for identifying and tracking the MAC addresses that are permanently associated with all network-capable digital devices. As mobile platforms emerged, tracking by permanent hardware identifiers has become routine. Telecommunications providers also have gotten into the act; most recently, Verizon customers were surprised to learn that Verizon had been tracking their online activities by means of a deeply embedded, invisible, and undeletable "supercookie" even after they had set their account preferences to reject such tracking (Chen and Singer 2015).

3.2 The Sensing Net

The initial extension of surveillance capability via cookie technology was an unintended consequence of the search for a viable protocol for commercial transactions, but subsequent extensions of surveillance capacity have been more deliberate. The primary vehicles for those extensions have been the marketplace shifts toward smart mobile devices, wearable computing, and the Internet of things. As a result of those developments, commercial information collection has become a nearly continuous condition. Communications networks are being transformed into sensing networks, organized around always-on mobile devices that collect and transmit an astonishingly varied and highly granular stream of information.

In the relatively short time since the first true smart phone was introduced by Motorola in 2004, Internet ready mobile devices have become ubiquitous and ordinary. In 2015, the Pew Research Center (2015) reported that 64% of U.S. adults own a smartphone. Even when used simply for one-to-one voice communications, mobile devices collect more information than tethered landlines do, for the simple reason that mobile devices use geolocation to route calls to their intended destinations. But smart mobile devices also collect and transmit text messages, Internet searches, social networking updates, personalized news and entertainment feeds, and interactions with dedicated apps for traffic, transit, shopping, investment and personal finance, fitness, and much more.

Personal information also flows through sensors embedded in ordinary artifacts and dispersed widely throughout the built environment. Transit passes and highway toll

transponders record daily travels; smart home thermostats, alarm systems, and building access cards create digital traces of comings and goings; and special-purpose "wearables" collect and upload biometric data to mobile apps that sync with cloud-based services. Fingerprint readers and facial recognition systems collect and process biometric information to authenticate access to devices, places, and services. Still other sensing systems, such as license plate readers and facial recognition technologies embedded in visual surveillance systems, are operated by the state.

Formally, commercial sensor networks require enrollment—apps must be installed and configured for location awareness, social sharing, push notifications, and the like. Particularly to those versed in the legal language of privacy and data protection, it might appear that legal construct enabling the ongoing construction of the sensor society remains the underlying right to control the processing of personal data and the data subject's consequent consent to collection and processing.

As a practical matter, though, information businesses have powerful incentives to configure the world of networked digital artifacts in ways that make enrollment seamless and near-automatic. Within the sensing net, practices of data collection are continuous, immanent, complex, and increasingly opaque to ordinary users. For some technologists and legal scholars, these characteristics have suggested an analogy to the autonomic nervous system, which automatically and responsively mediates basic physiological functions such as respiration and digestion (Cohen 2012; Hildebrandt and Rouvroy 2011; Kephart and Chess 2003). Like the autonomic nervous system, the sensing net is designed to operate invisibly and automatically, in a way that is exquisitely attuned to environmental and behavioral conditions. That means, however, that consent is being sublimated into the coded environment, and along the way it is being effectively redefined as a status that attaches at the moment of marketplace entry. Under those circumstances, the lawyerly emphasis on such things as disclosure, privacy dashboards, and competition over terms becomes a form of Kabuki theater that distracts both users and regulators from what is really going on.

The emergence of the sensing net and the ongoing sublimation of consent work both to generate large quantities of personal information and to make public domain status the default condition for the information that is generated. Or, as data broker Acxiom notes: "To drive value from the new opportunities presented by the Internet of Things, companies must be able to connect these new data feeds with their existing CRM [customer relations management] systems to distill enhanced insights and better understand their customer's needs beyond just the data from a connected device."[7] Unlike land, which exists in finite quantity, the supply of personal information is (in theory) subject to uncertainties: its seeming bounty depends heavily on both technical design and user agency. The sublimation of consent within the sensing net is a technique for supply chain management that is designed to ameliorate those uncertainties. It operates to call the biopolitical public domain into being and to define it as a zone of free appropriation.

[7] Kamal Tahir, "Marketing in the Internet of Things (IoT) Era," Acxiom Perspectives, April 9, 2015, http://www.acxiom.com/marketing-internet-things-iot-era/.

3.3 The Postcolonial Two-Step

It is tempting to understand the biopolitical public domain as a developed world phenomenon—or, less charitably, as a "first-world problem"—but it would be a mistake to do so. Today, the most valuable personal information is that collected from wealthier consumers in developed countries, who have readier access to networked information and communications technologies and more consumer surplus to be extracted. Additionally, among less privileged consumers and in less developed nations, lower economic resources and literacy levels translate into lower penetration rates for Internet use and mobile device ownership. Even so, the future of personal information processing is global. The drive to explore and colonize the global public domain of personal data has produced a pattern that I will call the postcolonial two-step: initial extensions of surveillance via a two-pronged strategy of policing and development, followed by a step back as the data harvests are consolidated and absorbed.

In some global contexts, data collection and processing initiatives have arisen within the context of policing operations. The bulk communications surveillance programs disclosed by Edward Snowden originated in an asserted need to combat terrorist threats originating abroad. On the ground, U.S. military battalions in Afghanistan and Iraq have used portable fingerprinting devices to gather biometric data from individuals suspected of ties to insurgency or simply seeking access to U.S. installations (Polk 2010; Seffers 2010). Some Latin American countries have begun using electronic access cards and biometric technologies—sourced from global technology companies—for policing and security purposes (Arteaga Botello 2012).

Critics of these and other initiatives have argued that they are incompatible with international human rights obligations and also have stressed the likelihood of "mission creep" into domestic policing. Both history and recent events suggest that those fears are well founded. In the USA, for example, biometric identification of both citizens and noncitizens has become an increasingly routine part of crossing the U.S. border and of the background checking process for a growing list of jobs and government benefits (Gates 2011). Both the Federal Bureau of Investigation and the New York City Police Department have conducted prolonged, intrusive surveillance of Muslim communities and leaders, relying on a range of surveillance techniques and, in the case of the FBI, on access to communications information provided by the NSA (Greenwald and Hussein 2014; Shamas 2013). For many, the special monitoring of Muslim populations evokes the climate that led eventually to Japanese internment during World War II. Moving earlier still, historian Alfred McCoy (2009) has documented the U.S. military's use of the Philippines as a test bed for surveillance techniques of various types, which then migrated back to the USA via the army's newly formed Military Intelligence Division during the years surrounding World War I.

In other global contexts, however, initiatives for personal data processing are framed as development projects aimed at improving the living standards and prospects of the world's least fortunate peoples. In India, the Aadhar system, which assigns an universal identification (UID) number based on biometric data, was conceived as a way of solving the enormous logistical challenges associated with providing government benefits (such as rice allotments and health services) to a population with high rates of poverty and illiteracy (Sathe 2011). Other initiatives attempt to compensate for the lack of developed financial and communications infrastructures using biometric and

wireless technology. In a number of African nations, financial institutions and telecommunications providers are conducting experiments with biometric identification cards that do double duty as banking tools, allowing direct access to various services but also generating streams of information that can be used to develop and market new services (Taylor 2016).

Among scholars and activists, a rich debate has unfolded about whether the Indian and African initiatives and others like them should be understood as empowering or commodifying (e.g., Dreze 2015; Punj 2012). The fairest answer to this question probably is that the evidence is mixed and that it is too early to say for certain. Yet some of the factors that make the impact of such projects difficult to assess are worth considering carefully. Development of surveillance infrastructures typically is contracted to multinational data processing companies (Taylor and Broeders 2015). The terms of those contracts are difficult to discover, and the countries in which such initiatives are sited may lack open-government laws that would force disclosure. In addition, such countries may have rudimentary data protection laws or weak enforcement (or both) and may be under pressure to accede to bilateral or multilateral free trade agreements mandating free flows of data across borders (Taylor 2016).

The distinctive pattern of the postcolonial two-step also is visible in policing and social welfare initiatives directed at wholly domestic populations within the USA. Felony convicts are subject to mandatory DNA collection, and many states and the federal government require DNA collection from felony arrestees. In a recent case upholding Maryland's felony arrestee testing law against a constitutional challenge, Supreme Court justices disagreed hotly about both the extent of the privacy interest in DNA and the potential for such laws to become templates for testing obligations directed at other segments of the population.[8] But biometric identification schemes already are in widespread use to identify and track recipients of government welfare programs (Gilliom 2001), to monitor certain categories of temporary visa recipients (Gates 2011), and in many other contexts involving vulnerable populations (Gilman 2012; Monahan 2006). Meanwhile, new data mining initiatives being developed, with the federal government's blessing, in the education and health care contexts are touted for their potential to improve the delivery of public services and funding.

Both globally and domestically, important questions remain about the trajectories of data flows for policing and data flows for development and about the relationships between the two kinds of data flows. Other questions concern the relationships between data collection efforts directed at favored and disfavored populations. Different kinds of surveillance generate different kinds of data streams, and the differences can lead to inferences when the data flows are combined. To take one example, some U.S. cities and states—colloquially known as "ban the box" jurisdictions—prohibit employers from asking job applicants about their arrest and imprisonment histories, but the information may be readily available from commercial sources, and the absence of certain other kinds of data (for example, unexplained gaps in debit or credit card history) can support an inference of imprisonment that obviates the need to ask. Finally, platform differences shape "ordinary" commercial surveillance practice. Both domestically and abroad, those of lower economic means are more likely to use smartphones for all of their Internet access (Pew Research Center 2015), and data collection via

[8] Maryland v. King, 133 S. Ct. 1958, 1968 (2013).

mobile devices is less transparent and less easily customized. The potential of relatively inexpensive mobile platforms to foster economic development and social inclusion is celebrated in the international development literature, but data collected from and about vulnerable populations also can be put to other, less salutary uses.

3.4 Secrecy as Enclosure

For both commentators and lawmakers, perhaps the most noteworthy attribute of the personal data economy has been its secrecy, which frustrates the most basic efforts to understand how the Internet search, social networking, and consumer finance industries sort and categorize individual consumers (e.g., Pasquale 2015). The networks of secret agreements that characterize the emerging personal data industry are entirely intelligible within the discourses of property and intellectual property law. They work to establish quasi-property entitlements enforceable against competitors in the event of misappropriation and against counterparties in the event of breach. Put differently, the networks of secret agreements that constitute markets for personal information are acts of enclosure. They represent strategies for consummating the appropriation of valuable resources from the (imagined) common.

Intellectual property scholars have invoked enclosure metaphorically to characterize large-scale legislative extensions of intellectual property rights (e.g., Benkler 1999; Boyle 2008). Inspired by Boyle's work, surveillance theorist Mark Andrejevic (2007) uses "digital enclosure" to denote the pervasive informational exposure that occurs within commercial surveillance environments and the consequent loss of control over self-articulation. Both uses of the metaphor situate acts of enclosure on a grand scale as a way of underscoring their connections to economic and political power.

But enclosure as a strategy also proceeds on a level that is more small-bore and ordinary than contemporary scholarly usage suggests. Information-related transactions routinely involve strategic uses of contractually mandated secrecy—uses that have situational, relationship-specific assertions of ownership and control as their avowed purpose. So, for example, participants in data-intensive industries routinely deploy trade secrecy law and contract law to achieve a measure of exclusive control over the information contained in their databases. Commercial data processors' heavy reliance on contractually enforced secrecy is consistent with this pattern. Acts of contractual enclosure are assertions of power in the Foucauldian sense: they represent a mode of action upon the actions of others (Foucault 1983, p. 220) that is both strategic and normative. Their immediate goal is to secure commercial and competitive advantage, but their more fundamental purpose is performative and directed toward stabilizing and reifying emerging patterns of data-related privilege.

Appropriation strategies based on contractually mandated secrecy are acts of legal entrepreneurship that both affirm and alter the legal status of collected information. Despite repeated efforts over the course of the twentieth century, data have proved powerfully resistant to formal, legislated propertization. The networks of secret agreements that characterize the emerging personal data industry step in where the map of formal legal entitlements ends, functioning simultaneously as self-interested programs for commercial advancement and assertions of normalizing authority. They both consummate processes of extraction and appropriation and constitute those processes as foreordained.

Data brokers' reliance on secrecy also underscores the difference between public domain and commons as resource governance strategies, and this in turn highlights a critical difference between commercial and research uses of personal data. Governance as commons entails rules for maintaining a resource as open to community members and also may involve rules imposing duties to use the resource sustainably and sanctions for abusing the privilege of membership (Benkler 2006; Frischmann 2012). Advocates for research uses of Big Data have sometimes argued (or have been happy to concede) that collections of personal data for scientific and nonprofit research should be governed as commons and that access to data should be subject to various data protection obligations (e.g., Toga and Dinov 2015). The public domain framing entails no comparable set of communal obligations; it functions and is intended to function as a backdrop for appropriation and private profit-seeking activity. To put the point a different way, although the new information capitalists have worked hard to construct the sociotechnical conditions for the biopolitical public domain, they have not done this so they could share equally in its fruits. Information capital is not monolithic, and the race to harvest and profit from the public domain of personal information is intensely contested.

In short, when considered in the context of the biopolitical public domain's productive logics, secrecy performs a function that is straightforward. Realizing the profit potential of commercial surveillance activity requires practices that mark data flows with indicia of ownership. The networks of secret agreements that characterize the emerging personal data industry represent strategies through which resources extracted from the biopolitical public domain are made to function as sources of competitive advantage and more broadly as appropriable assets.

4 From Raw to Cooked: a Political Economy of Patterns and Predictions

As it mobilizes sociotechnical activity to facilitate extraction and enclosure, the idea of a public domain of personal information also frames an approach to knowledge production that underwrites the processing of personal information on an industrial scale. That process begins with a set of conventions for cultivating and collecting personal data, within which the data to be collected are posited as "raw" even when they are elicited in carefully standardized fashion. Cultivated and extracted data enter an industrial production process during which they are refined to generate data doubles—information templates for generating patterns and predictions that can be used to target consumers with particular characteristics. Data doubles are not marketed individually but rather in groups; the participants in data markets trade in people the way one might trade in commodity or currency futures. The new data refineries infuse personally identifiable data with an epistemology optimized for surplus extraction—optimized for consuming consumers—and mark their outputs with indicia of legal privilege. The public domain construct supports that process from beginning to end.

4.1 Data Cultivars

The data harvested from individuals and fed into commercial systems of predictive analytics are framed as raw streams of observation to be gathered and then processed

and systematized. Thus, for example, Acxiom promises "meticulous data cleansing," while Oracle describes its "DaaS for Social" service as providing "categorization and enrichment of unstructured social and enterprise data."[9]

In scholarly and policy communities, the "raw data" framing has generated considerable debate. Scholars who study information systems argue that the "raw data" framing is not, and never could be, entirely accurate (e.g., Boyd and Crawford 2012; Gitelman 2013). Inevitably, data collection activities are structured by basic judgments about what to collect, what units of measurement to use, and what formats and codings will be used to store and mark the data that are collected. The new data mining techniques can move well beyond sorting customers into predefined categories, though, so an analyst looking for patterns is not constrained to search only in the ways for which any single dataset is coded. Some argue that this inherent dynamism undercuts the traditional scholarly narrative of surveillance as imposing an artificial and often invidious discipline and that automated data mining has at least the potential to offset human biases rather than reinforcing them (e.g., Zarsky 2013).

Particularly in light of the processes described earlier in this chapter, however, it is equally inaccurate to say that the data collected for processing just happen to be there. The flexible and adaptive techniques used within contemporary surveillance environments are—and are designed to be—productive of particular types of information. An algorithm for pattern detection and reinforcement may be formally agnostic about the content of a user's preferences—say, for burgers or sushi, for golf or bowling or for *Game of Thrones* or *ESPN College Football*—but it is not agnostic as to the kinds of information it collects and produces. As it operates, it generates new informational by-products that are themselves artifacts of the patterns of spending and attention with which its designers are concerned.

Processes of data collection in commercial surveillance environments are also and importantly participatory, often calling upon individual consumers to sort themselves by selecting various descriptors or categories that apply. Structured fields are informed by analysts' and marketers' sense of the types of patterns they are seeking and are intended to cultivate habits of self-identification in a very particular way. In Scott Lash's formulation, this process represents power becoming ontological (Lash 2007): power expressed not through hegemonic control of meaning but rather through techniques for making the crowd known to itself. The subjects of commercial surveillance are agents who find freedom of self-articulation through a focused and purposeful—and often playful—consumerism (Cohen 2016). To the extent that self-sorting requires sets of choices within structured fields, it effects a partial return to a more rigid patterning, undercutting the characterization of predictive analytics as protean and dynamic.

The various processes of harvesting and culling "raw" consumer personal data are usefully compared to the harvesting of raw materials within an industrial system of agriculture. Just as agriculture on an industrial scale demands grain varieties suited to being grown and harvested industrially (Pollan 2007), so the collection of personal information on an industrial scale inevitably adopts an active, curatorial stance

[9] Acxiom, "Data Solutions," http://www.acxiom.com/data-solutions/; Oracle, Press Release, "New Oracle Data Cloud and Data-as-Service Offerings Redefine Data-Driven Enterprise," July 22, 2014, http://www.oracle.com/us/corporate/pressrelease/data-cloud-and-daas-072214.

regarding the items to be gathered. Strains of information are selected and cultivated precisely for their durability and commercial value within a set of information processing operations. The data are both raw and cultivated, both real and highly artificial.

4.2 Data Refineries

After personal data have been cultivated and harvested, they are processed to generate patterns and predictions about consumer behavior and preferences. Like the practices of data collection and exchange discussed above, commercial data processing practices typically are shrouded in secrecy (Pasquale 2015). Here again, however, one does not need access to the technical details in order to understand the role that such processes play within the imagined narrative of the biopolitical public domain. In the emerging information economy, such processes function as information age refineries, processing inputs into the forms best suited for exploitation on an industrial scale.

Investigations of data-based systems of predictive analytics through the lens of privacy and data protection law typically criticize such systems for offering artificial and instrumental forms of personalization based on automated, externally determined logics. I have offered that characterization in my own work (e.g., Cohen 2012, 2013) and have no quarrel with it. The view from privacy scholarship, however, remains one that is informed by an individualistic frame of reference. Rights are tautologically individualistic, and scholarly fascination with social shaping also testifies powerfully to anxiety about subjectivity's absence.

The new data refineries, in contrast, operate on an entirely different scale. The agribusiness model again supplies a useful analogy: the processing of personal data within contemporary analytics-based commercial surveillance operations is comparable to the milling of corn and wheat to generate stable, uniform by-products optimized for industrial food production (Pollan 2007). Data refineries refine and massage consumer personal data to produce virtual representations—data doubles—optimized for modulating consumer behavior systematically. Data doubles correlate to identifiable consumers—they are sets of data that pertain to particular individuals and that can be used to simulate consumer behavior at a very high level of granularity—but their function within the emerging political economy of personal information is to subsume individual variation and idiosyncrasy within a probabilistic gradient. Their purpose is to make human behaviors and preferences calculable, predictable, and profitable *in aggregate*. As long as that project is effective on its own terms—an outcome that can be measured in hit rates or revenue increments—partial (or even complete) misalignments at the individual level are irrelevant.

Data doubles are, in other words, biopolitical in character: they are designed to enable the statistical construction, management of, and trade in populations. The idea of biopolitics more typically has been articulated in contexts involving the overt assertion of state power—thus, for example, when the government establishes performance metrics for allocating special education resources to some schoolchildren but not others, or when it promulgates standards for ideal body mass and recommended nutrition, we can identify a kind of biopolitical power at work (Foucault 2007; Mills 2016). Yet it is equally important to trace the emergence and articulation of biopolitical power in contexts where state authority plays a more general and constitutive role in constructing the conditions of possibility for private activity (see generally Gros 2016;

May and McWhorter 2016). Indeed, in the era of informational capitalism, with its accompanying ideology of neoliberal governmentality (Brown 2003; Lemke 2001), it is data refineries' very privateness that gives their outputs normative and epistemological authority.

Within the political economy of informational capitalism, the data refinery promises new ways of making knowledge about populations economically productive. That framing in turn suggests the importance of studying markets for the outputs of data refineries as markets—i.e., as economic phenomena with concrete institutional manifestations. Consider the agribusiness analogy again: Corn can be milled directly into flour for human consumption, but most of the principal markets for corn are the intermediate and derivative ones—markets for livestock feed and for chemical subcomponents, derived in industrial laboratories, that are used as sweeteners and preservatives (Pollan 2007). Those markets reflect extraordinary innovation of a sort but also operate to conceal the extent of our dependence on monoculture and to entrench that monoculture in ways that make addressing its external effects on human and environmental health extremely difficult. In similar fashion, data doubles have given rise to complex, derivative products traded in specialized markets with institutional lives of their own.

4.3 Data Markets

Understanding the markets for the outputs of data refineries requires probing beyond the economist's very general definition of a market as an economic system in which pricing and allocation of goods and services are determined as a result of the aggregate of exchanges between participants, without central direction or control. That definition treats the market mechanism as a black box; it begs both the question of what might come to qualify as a good or service and that of how transactions might be made intelligible as exchanges. An adequate description of the origins and operation of emerging markets in personal data requires investigation of precisely those questions.

As a general, abstract matter, markets are institutional structures for calculated exchanges. As elaborated by Callon and Muniesa (2005), this definition has three principal parts. First, a functioning market requires a subject matter that is capable of being valued so that it can be traded. Put differently, that subject matter must be reconceived as a "calculable good": a good detached from its context in a way that enables it to be objectified, manipulated, and valued. Because calculable goods must be marketed to prospective buyers, buyers participate in that process, whether by serving as audiences for marketing campaigns or more actively by providing feedback or other input. Second, a functioning market requires a widely distributed "calculative agency": a framework that mobilizes calculative power using a set of common techniques and methods. For example, the supermarket system of price labels, coupons, and barcode scanners and the online "shopping cart" each embed a type of calculative agency that enables market participants to participate in the valuation of calculable goods. Calculative agency may be distributed asymmetrically—consumers, for example, do not play an active role in determining the price of shampoo but do participate in its purchase and in the consumption of advertising that positions shampoo as a desirable purchase. Third, a functioning market requires a commonly understood institutional structure within which exchanges can occur. The institutional structure must be capable

of bringing would-be participants together and enabling them to engage in what Callon and Muniesa call a "calculated encounter": an encounter generally mediated by distributed, materially embedded techniques and practices that all parties understand as transactional. Thus, for example, the procedures followed on the trading floor of the New York Stock Exchange and in Japanese tuna markets (Feldman 2006) each command unquestioned, deeply embedded assent as ways of ordering distribution and allocation.

Although the terms and conditions of business-to-business transactions over consumer personal information have proved astonishingly difficult to locate and bring into the light of day, the fact that they exist (to the tune of billions of dollars) speaks volumes about the emergence of conventions for defining personal information by-products as calculable goods. The existence of a billion-dollar market in personal information processing also testifies to the emergence of a calculative agency that is widely distributed among market participants and an institutional framework for structuring their calculated encounters.

To understand the process by which calculable goods are defined in markets for personal information, however, we must contend with the fact that the entities to be detached and made calculable are data doubles deriving from consumers themselves. Although it is customary in public-facing rhetoric about personal data collection and processing to refer to consumers as individuals with singular wants and needs that data collection helps marketers to fulfill, that framing does not align with what we are coming to understand about the nature and operation of data markets. Notably, Callon and Muniesa (2005) use the frame of singular wants and needs to denote not actual personalization but rather the performance of personalization via marketing strategy. In their terminology, marketers seek to "singularize" their goods for consumers and often may do so by appealing to ideals of individualization. That framing aptly describes public-facing rhetoric about personal data processing, which is designed to stabilize the data supply chain by encouraging consumer participation.

By the same token, marketers of data-based predictive analytics also have services to singularize for their target markets, but that process does not require actually singling out particular individuals as desirable recipients of marketing appeals. Instead, data-based predictive analytics operate to "probabilize" consumers, producing tranches of data doubles with probabilistically determined purchasing and risk profiles (Elmer 2013; Hildebrandt 2015; Zuboff 2016). Businesses of all sorts can then purchase those tranches as inputs (refined materials) to their own production processes. Those processes have consumers as their targets, but they are not consumer-centered. Instead, purchased access to probabilized tranches of data doubles increasingly is believed to be the most profitable way of framing other calculated exchanges over other goods and services, such as consumer electronics, information services, mortgage loans, consumer credit, and travel. Using the information supplied by the new data refineries, marketers may singularize those goods and services for target populations of consumers more effectively.

From the consumer perspective, the results generated by calculated exchanges between data refineries and their customers may appear as reduced search and transaction costs. In the age of infoglut (Andrejevic 2013), we all seek strategies for cutting through the clutter; to the extent that profiling and targeted marketing reproduce the results of that process, they can appear to produce significant, tangible benefits. Those

strategies, however, have ripple effects on other market institutions; and that is exactly their point. Both the material logics of appropriation discussed in the previous section and the epistemological logics discussed in this section operate to submerge important features of transactions in business-to-consumer markets, producing calculated exchanges that are increasingly etiolated.

4.4 From Public to Proprietary: Consuming Consumers

Scholarly investigations of techniques for processing personal information tend to frame the use of data-based analytics as a knowledge production process with secondary economic justice implications, rather than as an economic and legal-institutional process with secondary knowledge production implications. Those critiques are trenchant, and yet there is an important way in which they miss the point. The data refinery is only secondarily an apparatus for producing knowledge. It is principally an apparatus for producing wealth. Its actions express both a distinctive logic of economic accumulation (Zuboff 2015) and an equally distinctive logic of legal privilege.

The new data refineries offer powerful, high-speed techniques for matching people not only with goods and services but more precisely with particular prices and feature packages calibrated for surplus extraction. The techniques operate on "raw" personal data to produce "refined" data doubles and use the data doubles to generate preemptive nudges that, when well executed, operate as self-fulfilling prophecies, producing consummated transactions over the offerings already judged to be most likely to appeal. Academic commentary on the use of preemptive nudges in advertising and content provision (Hildebrandt 2015; Kerr and Earle 2013) has paid relatively little attention to the question of their economic function, but that function is fundamental: Preemptive nudges work to maintain and stabilize the available pool of consumer surplus so that it may be more predictably identified and easily extracted.

This description of the personal data economy, which posits consumers as resources to be themselves cultivated, processed, and consumed, has a science fiction quality to it, and yet within intellectual property circles its form is entirely commonplace. In 1984, John Moore sued the Regents of the University of California and a UCLA doctor who had treated his leukemia for conversion (wrongful appropriation) of his personal property. The property identified in his complaint was his cancerous spleen, which had been removed from his body and used to develop a valuable, patented cell line. The lawsuit reached the California Supreme Court, which rejected Moore's conversion theory on the ground that diseased tissue removed from the human body could not be the subject of a property interest (though it allowed Moore to maintain an action for failure of informed consent).[10] Among lawyers, the *Moore* opinion is famous. It is routinely included in first-year property casebooks, where it stands for the principle that anti-commodification values can (sometimes) prevent the propertization of human tissue. But the court did not hold that human tissue could not be the subject of any proprietary claims. Rather, it contrasted Moore's claim to that of the research scientists who had labored to develop the patentable by-product. And, even as it took for granted the wisdom of granting patents on medical research by-products, it worried fretfully about the costs to innovation of allowing proprietary claims to the raw materials used in medical research.

[10] Moore v. Regents of the University of California, 793 P.2d 479 (Cal. 1990).

One can trace a similar elaboration of relative privilege and disentitlement in the evolving debate about the future of fair information practices in the era of pervasive commercial surveillance. In regulatory proceedings and in the media, the data processing industries have advanced a carefully crafted narrative that links data processing with "innovation" and positions privacy and "innovation" as fundamentally and intractably opposed. The resulting "surveillance-innovation complex" (Cohen 2016) powerfully shapes prevailing perceptions of feasible regulatory options. Even while asserting their own authority, regulators have embraced the framing idea of a balance between opposing goods and have looked to illusory notions of user choice to provide a way out of the resulting dilemma.[11] Meanwhile, commentators concerned to preserve the benefits of so-called Big Data worry that a right to withdraw one's data from databases, if widely exercised, would compromise the utility of those databases as resources for pattern identification (e.g., Tene and Polonetsky 2012).

Meanwhile, and revealingly, the contest to develop newer, more direct, and more effective extractive techniques rages on. Data brokers proudly tout their "unprecedented," "proprietary," and sometimes "patented" analytic techniques.[12] Claims like this situate ownership of personal data at the heart of the data refinery, vesting it in those who (supposedly) create value where none previously existed. They work to create and perpetuate a narrative of romantic authorship that unfolds in counterpoint to that of the public domain and that is old and familiar (Boyle 2008; Chander and Sunder 2004). Other narratives about innovative exploitation of the biopolitical public domain locate romance in the technologies themselves—in their power to find patterns, unlock new sources of competitive advantage, and enable new strategies for surplus extraction and accumulation (Cohen 2013).

In short, there is more at stake here than a new model of knowledge production. The idea of a public domain of personal information alters the legal status of the inputs to and outputs of personal data processing. In that sense, it is relational and distributive: it both suggests and legitimates a pattern of appropriation by some, with economic and political consequences for others. In the wake of those powerful shaping effects, both proposal for additional "regulation" and high-profile enforcement actions by regulators seem always to do too little and come too late.

5 Conclusion

The idea of a public domain of personal information sets in motion a familiar and powerful legal and economic just-so story. It naturalizes practices of appropriation by data processors and data brokers, positions the new data refineries and their outputs as

[11] See, for example, U.S. Federal Trade Commission, "Protecting Consumer Privacy in an Era of Rapid Change" (2012), http://www.ftc.gov/os/2012/03/120326privacyreport.pdf; White House, "Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy" (2012), http://www.whitehouse.gov/sites/default/files/privacy-final.pdf.

[12] For some examples, see Oracle, Press Release, "New Oracle Data Cloud and Data-as-Service Offerings Redefine Data-Driven Enterprise," July 22, 2014, http://www.oracle.com/us/corporate/pressrelease/data-cloud-and-daas-072214 (unprecedented intelligence"); Spokeo, "About," http://www.spokeo.com/about ("proprietary merge technology"); Intelius, "About," http://corp.intelius.com/ ("proprietary genomic technology"); ID Analytics, "Company Overview," http://www.idanalytics.com/company/ ("patented analytics").

sites of legal privilege, and elides the connections between information and power. That process subtly and durably reconfigures the legal and economic playing field, making effective regulation of its constituent activities more difficult to imagine.

The emergence of the biopolitical public domain thus raises questions of both political and economic justice, and the two are tightly entwined. Legal and surveillance studies scholars (e.g., Andrejevic 2007, 2013; Cohen 2013; Hildebrandt 2015; Pasquale 2015) have argued that surrendering control of the information environment to opaque, immanent data processing practices amounts to surrendering control over both self-development and self-government. The impact on markets is equally profound. The legal-institutional construct of the biopolitical public domain alienates consumers from their own data as an economic resource and from their own preferences and reservation prices as potentially equalizing factors in market transactions, producing a set of wholly nontransparent exchange institutions that reconfigure demand to match supply. It seeks, in wholly unironic fashion, a commercial future in which consumer surplus is extracted "from each according to his abilities," while goods and services flow "to each according to his [manufactured] needs" (Marx 1996, p. 215; see also Fourcade and Healy 2016).

At least according to theory, in a capitalist society, market transactions function as an essential mode of governance. The construct of the biopolitical public domain sits in fundamental tension with that market-libertarian ideal. Despite the popularity of transactional consent as a frame for neoliberal policy discourse, the emerging surveillance economy leaves consent—and, for that matter, volition—with very little work to do. It reflects a biopolitics of crowds, through which the "common productive flesh of the multitude has been formed into the global political body of capital" (Hardt and Negri 2004, p. 189). If a different future is desired, for privacy and data protection or more generally for markets, this is the point at which policy debates need to begin.

Acknowledgements My personal thanks go to Mireille Hildebrandt and Frank Pasquale and participants in the Fordham Center on Law & Information Policy faculty workshop, the Georgetown-Maryland Privacy Faculty discussion group, the 2015 Privacy Law Scholars Conference for their helpful comments, and Aislinn Affinito, Peter Gil-Montllor, Alex Moser, and Sean Quinn for research assistance.

References

Acquisti, A., Brandimarte, L. E., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science, 347*(6221), 509–514.

Andrejevic, M. (2007). *iSpy: surveillance and power in the interactive era*. Lawrence: University Press of Kansas.

Andrejevic, M. (2013). *Infoglut: how too much information is changing the way we think and know*. New York: Routledge.

Arteaga Botello, N. (2012). Surveillance and urban violence in Latin America. In K. Ball, K. D. Haggerty, & D. Lyon (Eds.), *Routledge handbook of surveillance studies* (pp. 259–266). New York: Routledge.

Benkler, Y. (1999). *Free as the Air to Common Use: First Amendment Constraints on Enclosure of the Public Domain*. New York University Law Review, *74*(2), 354–445.

Benkler, Y. (2006). *The wealth of networks: how social production transforms markets and freedom*. New Haven: Yale University Press.

Boyd, D., & Crawford, K. (2012). Critical questions for big data: provocations for a cultural, technological, and scholarly phenomenon. *Information, Communication & Society, 15*(5), 662–679.

Boyle, J. (2008). The second enclosure movement and the construction of the public domain. *Law and Contemporary Problems, 66*(1–2), 33–74.
Brown, W. (2003). Neo-liberalism and the end of liberal democracy. *Theory & Event, 7*(1),http://muse.jhu.edu/journals/theory_&_event/.
Callon, M., & Muniesa, F. (2005). Peripheral vision: markets as calculative collective devices. *Organization Studies, 26*(8), 1229–1250.
Castells, M. (1996). The Rise of the Network Society. New York: Wiley-Blackwell.
Chander, A., & Sunder, M. (2004). The romance of the public domain. *California Law Review, 92*(5), 1331–1373.
Chen, B. X. & Singer, N. (2015). Verizon wireless to allow complete opt-out of mobile "supercookies". *New York Times Online*, Jan. 30, 2015, http://bits.blogs.nytimes.com/2015/01/30/verizon-wireless-to-allow-complete-opt-out-of-mobile-supercookies/?_r=2.
Cohen, J. E. (2012). *Configuring the networked self: law, code, and the play of everyday practice*. New Haven: Yale University Press.
Cohen, J. E. (2013). What privacy is for. *Harvard Law Review, 126*(7), 1904–1933.
Cohen, J. E. (2016). The surveillance-innovation complex: the irony of the participatory turn. In D. Barney, G. Coleman, C. Ross, J. Sterne & T. Tembeck (Eds.), *The participatory condition in the digital age* (pp. 207–226). Minneapolis: University of Minnesota Press.
Deleuze, G. (1995). Postscript on control societies. *In Negotiations 1972–1990 (trans. Martin Joughin)*. New York: Columbia University Press.
Dreze, J. (2015). Unique identity dilemma, *The Indian Express*, Mar. 19, 2015, http://indianexpress.com/article/opinion/columns/unique-identity-dilemma/.
Elmer, G. (2013). IPO 2.0: the Panopticon goes public. *Media Tropes, 4*(1), 1–16.
Feldman, E. A. (2006). The tuna court: law and norms in the world's premier fish market. *California Law Review, 94*(2), 313–369.
Feller, D. (1984). *The public lands in Jacksonian politics*. Madison: University of Wisconsin Press.
Foucault, M. (1978). *The history of sexuality, vol. 1, an introduction (trans. Robert Hurley)*. New York: Random House.
Foucault, M. (1983). Afterword: the subject and power. In H. L. Dreyfus & P. Rabinow (Eds.), *Michel Foucault: beyond structuralism and hermeneutics* (2nd ed., pp. 208–228). Chicago: University of Chicago Press.
Foucault, M. (2007). *Security, territory, population: lectures at the College de France 1977–78 (trans. Graham Burchell)*. New York: Picador.
Fourcade, M. & Healy, K. (2016). Seeing like a market. *Socio-Economic Review*, 14(4), [pages], doi: https://doi.org/10.1093/ser/mww033.
Frischmann, B. M. (2012). *Infrastructure: the social value of shared resources*. New York: Oxford University Press.
Gandy Jr., O. H. (1993). *The panoptic sort: a political economy of personal information*. Boulder: Westview.
Gates, P. W. (1996). *The Jeffersonian dream: studies in the history of American land policy and development*. Albuquerque: University of New Mexico Press.
Gates, K. A. (2011). *Our biometric future: facial recognition technology and the culture of surveillance*. New York: New York University Press.
Gilliom, J. (2001). *Overseers of the poor: surveillance, resistance, and the limits of privacy*. Chicago: University of Chicago Press.
Gilman, M. E. (2012). The class differential in privacy law. *Brooklyn Law Review., 77*(4), 1389–1445.
Gitelman, L. (Ed.). (2013). *"Raw data" is an oxymoron*. Cambridge: MIT Press.
Greenwald, G., & Hussein, M. (2014). Meet the Muslim-American leaders the FBI and NSA have been spying on. *The Intercept*, July 9, 2014, https://firstlook.org/theintercept/2014/07/09/under-surveillance/.
Gros, F. (2016). Is there a biopolitical subject? Foucault and the birth of biopolitics. In V. W. Cisney & N. Morar (Eds.), *Biopower: Foucault and beyond* (pp. 259–273). Chicago: University of Chicago Press.
Hardt, M., & Negri, A. (2004). *Multitude: war and democracy in the age of empire*. New York: Penguin.
Hildebrandt, M. (2015). *Smart technologies and the end(s) of law*. Northampton: Edward Elgar.
Hildebrandt, M., & Rouvroy, A. (Eds.). (2011). *Law, human agency and autonomic computing*. New York: Routledge.
Kephart, J. O., & Chess, D. M. (2003). The vision of autonomic computing. *Computer, 36*(1), 41–50.
Kerr, I., & Earle, J. (2013). Prediction, preemption, presumption: how big data threatens big picture privacy. *Stanford Law Review Online, 66*(2013), 65–72.
Kristol, D. M. (2001). HTTP cookies: standards, privacy, and politics. *ACM Transactions on Internet Technology, 1*(2), 151–198.

Lash, S. (2007). Power after hegemony: cultural studies in mutation? *Theory Culture & Society, 24*(3), 55–78.
Lemke, T. (2001). "The birth of bio-politics": Michel Foucault's lecture at the College de France on neo-liberal governmentality. *Economy and Society, 30*(2), 190–207.
Litman, J. (1990). The public domain. *Emory Law Journal, 39*(4), 965–1023.
Locke, J. (1947). *Two treatises on government*. In T. I. Cook (ed.). New York: Hafner Publishing Co.
Manning, R. D. (2000). *Credit card nation*. New York: Basic Books.
Marx, Karl. 1996. Critique of the Gotha program. In Terrell Carver (Ed. & Trans.), Marx: later political writings (pp. 208–226). New York: Cambridge University Press.
May, T., & McWhorter, L. (2016). Who's being disciplined now? Operations of power in a neoliberal world. In V. W. Cisney & N. Morar (Eds.), *Biopower: Foucault and beyond* (pp. 245–258). Chicago: University of Chicago Press.
McCoy, A. (2009). *Policing America's empire: the United States, the Philippines, and the rise of the surveillance state*. Madison: University of Wisconsin Press.
Mills, C. (2016). Biopolitics and the concept of life. In V. W. Cisney & N. Morar (Eds.), *Biopower: Foucault and beyond* (pp. 82–101). Chicago: University of Chicago Press.
Monahan, T. (Ed.). (2006). *Surveillance and security: technological politics and power in everyday life*. New York: Routledge.
Nail, T. (2016). Biopower and control. In N. Morar, T. Nail, & D. W. Smith (Eds.), *Between Deleuze and Foucault* (pp. 247–263). Edinburgh: University of Edinburgh Press.
Pasquale, F. (2015). *The black box society: the secret algorithms that control money and information*. Cambridge: Harvard University Press.
Pew Research Center. (2015). *The smartphone difference*. April 2015, http://www.pewinternet.org/2015/04/01/us-smartphone-use-in-2015.
Polanyi, K. (1957). *The great transformation: the political and economic origins of our time*. Boston: Beacon Press.
Polk, T. (2010). *Handheld device helps soldiers detect the enemy*, Jan. 14, 2010; http://www.army.mil/mobile/article/?p=32913.
Pollan, M. (2007). *The omnivore's dilemma: a natural history of four meals*. New York: Penguin.
Punj, S. (2012). A number of changes. *Business Today*. Mar. 4, 2012, http://businesstoday.intoday.in/story/uid-project-nandan-nilekani-future-unique-identification/1/22288.html.
Sathe, V. (2011). The world's most ambitious ID project. *Innovations, 6*(2), 39–65.
Seffers, G. I. (2010). U.S. Defense Department expands biometrics technologies, information sharing. *SIGNAL Magazine*, Oct 2010, http://www.afcea.org/content/?q=us-defense-department-expands-biometrics-technologies-information-sharing.
Shamas, D. (2013). Where's the outrage when the FBI targets Muslims? *The Nation*, Oct. 31, 2013, https://www.thenation.com/article/wheres-outrage-when-fbi-targets-muslims/.
Solove, D. J., & Hartzog, W. (2014). The FTC and the new common law of privacy. *Columbia Law Review, 114*(3), 583–676.
Taylor, L. (2016). Data subjects or data citizens? Addressing the global regulatory challenge of big data. In M. Hildebrandt & B. van den Berg (Eds.), *Freedom and property of information: the philosophy of law meets the philosophy of technology* (pp. 81–105). New York: Routledge.
Taylor, L., & Broeders, D. (2015). In the name of development: power, profit and the datafication of the global south. *Geoforum, 64*(2015), 229–237.
Tene, O., & Polonetsky, J. (2012). Privacy in the age of big data: a time for big decisions. *Stanford Law Review Online, 64*(2012), 63.
Toga, A. W. & Dinov, I. V. (2015). Sharing big biomedical data. *Journal of Big Data*, 2:7, doi:10.1186/s40537-015-0016-1.
Varian, H. R. (2014). Beyond big data. *Business Economics, 49*(1), 27–31.
Willis, L. E. (2013). When nudges fail: slippery defaults. *University of Chicago Law Review, 80*(3), 1155–1229.
Willis, L. E. (2015). Performance-based consumer regulation. *University of Chicago Law Review, 82*(3), 1309–1409.
Zarsky, T. (2013). Transparent predictions. *University of Illinois Law Review, 2013*(4), 1503–1570.
Zuboff, S. (2015). Big other: surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology, 30*, 75–89.
Zuboff, S. (2016). The secrets of surveillance capitalism. *Frankfurter Allgemeine Zeitung*, Mar. 5, 2016, http://www.faz.net/aktuell/feuilleton/debatten/the-digital-debate/shoshana-zuboff-secrets-of-surveillancecapitalism- 14103616.html.