Between Truth and Power (New York: Oxford Univ. Press, 2019)

Chapter 2
The Biopolitical Public Domain

"In the beginning all the World was America."
John Locke, Second Treatise of Government, §49.

Chapter 1 described the emergence of the platform as the core organizational logic of the political economy of informational capitalism. Platforms have become both key drivers of the datafication of important resources and active legal entrepreneurs, pursuing powerful strategies for ensuring their continued access to and de facto control of the data on which they rely. That exploration, however, also raised an important question that sits outside the frame of propertization-through-control and that concerns the origins of the presumptive entitlement that platforms and other information businesses assert to appropriate and use data flows extracted from people. That presumptive entitlement is the subject of this chapter.

Scholarship on the relationship between law and the collection and processing of personal data typically considers such activities as raising problems of privacy or data protection, and typically has focused on regulation of such activities after the fact. But the legal framework within which collection, processing, and use of personal data occur is not simply a reactive framework, nor is it simply concerned with the relationship between commercial or law enforcement activities and privacy. The data flows extracted from people play an increasingly important role *as raw material* in the political economy of informational capitalism. Personal data processing has become the newest form of bioprospecting, as entities of all sizes—including most notably both platforms and businesses known as data brokers—compete to discover new patterns and extract their marketplace value.

Understood as processes of resource extraction, the activities of collecting and processing personal data require an enabling legal construct. This chapter 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 data extraction and processing constitute a new type of public domain, which I will call the *biopolitical public domain*: a source 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 data 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.

A public domain is not a naturally occurring phenomenon. It is first and foremost an idea: a culturally situated way of understanding patterns of resource ownership and availability. But a public domain also is much more than an idea. The construct of a public domain both designates particular types of resources as available and suggests particular ways of putting them to work. In Hohfeldian terms, a public domain is a zone of legal privilege: it demarcates conduct as to which no one has a right to object. It thereby legitimates the resulting patterns of appropriation and obscures the distributive politics in which they are embedded.[1] The biopolitical public domain conforms to these patterns, constituting the field for appropriation and use of personal data in two complementary and interrelated ways. First, it constitutes personal data 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 data 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. It thereby catalyzes the emergence of a complex set of economic and social relations.

My purpose in naming the biopolitical public domain and exploring its material and conceptual entailments is to construct a genealogy of legal privilege-in-the-making. The emerging patterns of privilege and disentitlement now coalescing around the construct of the biopolitical public domain have far-reaching implications in the domains of both political economy and law. They undergird new business-to-business markets based on patterning, prediction, and targeted surplus extraction, and those markets profoundly alter other economic and social relationships. As legal institutions confront choices about whether to validate or constrain the practices that make such markets possible, it is important to recognize the extent to which law is already implicated in the construction and assertion of information power.

Logics of Abundance and Extraction

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 an act of imagination tailored to the political economy of informational capitalism; it constitutes the field of opportunity for a particular set of information-based extractive activities.

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.[2] Later, for the fledgling government of the United States, 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.[3] The copyright and patent regimes that emerged during the nineteenth century in Europe and the United States 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 resources in the intellectual public domain, but resources in the public domain may be freely appropriated as inputs to 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 put it in 1690, "in the beginning all the World was America."[4] 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. Legal scholars Anupam Chander and Madhavi Sunder, 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.[5]

The idea of a public domain thus reflects an implicit distributive politics, with important, real-world consequences for the distribution of economic wealth. The idea of the biopolitical public domain conforms to that pattern.

Contemporary descriptions of the commercial future of personal data processing contain numerous examples of framing in terms of abundance and infinite possibility. In marketing brochures and prospectus statements, information businesses of all sorts describe in glowing terms the ways that processing of data about people will open new and profitable lines of exploration. Data broker Intelius boasts: "Intelius has a robust and proprietary technology platform that gathers over 20 billion public records from a large network of publicly- and commercially-available sources." TowerData (formerly Rapleaf) promises "80% of email or postal addresses in batch or via a real-time API," and CoreLogic touts its access to "more than 4.5 billion records" and its focus on "turning mountains of data into valuable insights," while according to Recorded Future, it

"continuously processes billions of data points in multiple languages from technical, open, and closed (dark web) sources."[6] These optimistic pronouncements, which herald the dawn of a new age of data science, constitute the ever-expanding universe of personal data 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."[7] Google Chief Economist Hal Varian 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."[8] 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 United States 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.

Imagining the universe of personal data as a commons ripe for exploitation 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.

Prologue: Fair Credit Reporting and Walled Gardens

The personal data processing economy derives its structure partly from the activities of the platform businesses described in Chapter 1 and partly from those of a different group of information businesses known as data brokers. Today, the commercial data broker industry is a multi-billion dollar industry that, according to a 2013 study by the U.S. Senate Committee on Commerce, Science, and Transportation, "largely operates hidden from public view."[9] Its origins, however, are both more modest and more public. As we saw in Chapter 1, platforms trace their roots to developments in advertiser-driven target marketing that began in the early twentieth century. The data broker industry originated in practices of customer profiling and target marketing developed by and for members of the financial services industries—and in the empty spaces left by incomplete legal regulation of those practices.

Ironically, one impetus for the emergence of consumer profiling and target marketing within the financial services industry was a law intended to protect consumers. By the mid-twentieth century, both consumer advocates and legislators had become alarmed by the free-wheeling nature of the emerging credit reporting industry. Lenders and third-party consultants were building dossiers that demonstrated scant regard for

accuracy and disseminating them with even scanter regard for the value of confidentiality and the potential for harm. The Fair Credit Reporting Act of 1970 (FCRA) created both substantive and procedural safeguards, including limits on the purposes for which a "consumer report" could be provided, informed consent provisions for the release of certain kinds of information, and procedures by which consumers could gain access to the records compiled by consumer reporting agencies and correct any errors.[10]

The FCRA's drafters, however, also had other goals in mind. The law imposed no duty on consumer reporting agencies to verify reported information or reconcile discrepancies between conflicting reports, but instead simply required them to respond to consumer complaints once raised. It provided automatic, statutory damages only for willful violations, and preempted any state law causes of action that might have imposed stricter duties or more significant deterrent liability. In short, the much-heralded federal law with "fair" in its title was designed with the significant purpose of ensuring smooth sailing for the fledgling consumer reporting industry.[11] In that purpose it succeeded. As electronic processes for credit reporting and approval emerged, the uniform federal limitation on liability and the relatively weak, post hoc guarantees of procedural fairness facilitated the emergence of nationwide, automated credit reporting agencies and a vast and profitable consumer credit industry.

Notably, the drafters of the FCRA did not attempt to develop a new, comprehensive definition of a "consumer reporting agency," but instead employed recursive definitions: consumer reports are communications of credit-related information by consumer reporting agencies, while consumer reporting agencies are entities that assemble and evaluate consumer credit information for the purpose of furnishing consumer reports.[12] That approach likely made sense for both practical and political reasons; it avoided the difficult task of generating consensus on the precise coverage of a sweeping new law intended to govern still-emerging entities and practices. At any rate, the project of amassing comprehensive, searchable nationwide databases still confronted large logistical and technical challenges. All parties seem to have assumed that when the dust settled after an inevitable period of consolidation, consumer reporting agencies would be few in number and easy to identify by the nature of the reports their resources enabled them to prepare. The statutory circularity, however, created an important point of entry for the nascent consumer profiling industry. From early on, the structure of the statute's definitions seems to have encouraged both consumer reporting agencies and other entities to experiment with data-based products and services that could be offered for sale without triggering the FCRA's requirements.[13]

The FCRA also did not impose any special legal obligations on financial institutions that submitted information about consumers' payment behavior to consumer reporting agencies. Submitters, Congress likely assumed, would not be in position to compile comprehensive reports using only the discrete items of information each possessed. As we saw in Chapter 1, however, one consequence of the intensified financialization that began in the late twentieth century was a rapid increase in consumer reliance on revolving credit, and credit card issuers' proprietary databases grew commensurately. Jockeying for competitive advantage in an increasingly crowded field that now included American Express charge cards, major payment brand networks, and

independent credit issuers, card issuers began to mine their databases in an effort to identify different market segments and possible co-branding opportunities.[14]

One important structural limitation constrained experimentation with consumer profiling. As practices of consumer profiling evolved within the consumer reporting and credit card industries, the databases used to generate consumer reports and profiles remained walled gardens. The three major consumer reporting agencies received data directly from banks, credit card companies, and other financial institutions that had preexisting relationships with consumers and followed statutorily prescribed procedures in granting access to the reports they compiled. Consumer credit issuers built databases of their own cardholders' transactions. As the twentieth century drew to a close, however, the information-gathering landscape changed decisively.

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.[15] 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.[16]

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 activity. 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 dramatic 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. By mid-1996, when articles in the *Financial Times* and the *San Jose Mercury News* revealed to the general public the existence of cookies for online tracking, experiments with the use of cookies as persistent identifiers were already underway.[17] That same year, the Federal Trade Commission (FTC) held public hearings about "consumer privacy in the global information infrastructure" during which the use of cookies to collect information about internet users was a topic of lively discussion.[18]

Over the ensuing decade, the increasing public and regulatory scrutiny of cookies did nothing to dampen commercial enthusiasm for the technology. As Chapter 1 described, new capabilities for intermediation and legibility intersected with the pursuit of commercial viability in an increasingly fragmented media environment. Advertisers

who might provide revenue wanted results and so, increasingly, did users. Personalized tracking seemed the logical way to satisfy both imperatives.

As the push for more user control intensified, Netscape and other browser developers began to build greater transparency and control into subsequent iterations of their browsers. At the same time, however, the commercial web resisted. 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," for surreptitiously collecting information about internet users' behavior.[19] The IETF working group had identified the privacy issues raised by cookies very early on, but 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. More generally, the IETF standards process had not previously experienced intensive public policy scrutiny. Working group members unused to evaluating and responding to political and policy objections had difficulty bringing the standards process to closure, and the delay allowed the more minimal standard to become entrenched within industry practice.[20]

Meanwhile, new platform-based environments for social sharing and massively multiplayer gaming were taking shape in ways that relied on techniques for keeping track of users. The earliest online communities were organized around chat rooms, listservs, and communal bulletin boards, and had neither the desire nor the capability for built-in surveillance. Similarly, the original online massively multiplayer games were not-for-profit enterprises organized around communities of enthusiasts rather than around the quality of the multimedia experiences they provided. In the late 1990s and early 2000s, however, the first true multimedia gaming platforms and social networking platforms began to emerge: graphically rich, hypertext-based environments that enabled customizable member profiles and relied on cookies to manage login information.[21] As they moved beyond the startup phase and sought stable sources of financing from capital markets, both kinds of platforms gradually became entangled within the biopolitical public domain's commercial and extractive logics. In particular, venture capital investors encouraged high tech startups to pursue business models that might generate the revenue streams needed to attract additional capital.[22]

Among the companies on the receiving end of investor pressure was Silicon Valley darling Google, which was in search of a formula for ensuring its continued survival following the end of the "dot-com bubble," and which had already built the most powerful engine for online search that the world had ever seen. Gradually, following the lead of its digital advertising team, it began developing, patenting, and acquiring new methods for generating online advertising revenues that relied on comprehensive information about users to target ads.[23] In that effort it was soon joined by new kid on the block Facebook, which was working to develop methods of monetizing a new form of digital asset that it called the "social graph."[24]

At the same time, both old and new data brokers were developing the capability to combine multiple databases and search across them to amass more complete dossiers on

individuals. As a wider variety of data began to be digitized, automated, and offered for sale or license—including directory listings, property records, tort judgments, divorce decrees, arrest records, and many more—data brokers were well positioned to acquire and exploit them.[25] Data brokers and emerging platform firms also contracted with or acquired new Web-based analytics firms that relied on cookies and web bugs to monitor users' activities, gathering valuable information that could be used to personalize content, sell ads, and generate revenue streams in transactions with subscribing clients. Google and Facebook pursued especially aggressive acquisition strategies, targeting both established and start-up firms and assimilating both competing and complementary functionalities.[26]

Last but not least, digital advertising ventures, data brokers, and emerging digital platform firms began to exploit new capabilities for data analysis. Those capabilities combined new configurations of information processing hardware capable of sifting, sorting, and interrogating vast quantities of data in very short times with new automated techniques for identifying patterns, distilling the patterns into predictions, and continually adjusting the patterns and predictions in response to new data. The result, popularized under the moniker "Big Data," was a fast-evolving group of techniques for converting voluminous, heterogeneous flows of physical, transactional, and behavioral information about people (or about anything else) into a particular, highly data-intensive type of knowledge.[27]

Efforts to extend consumer protection frameworks to encompass the new developments were largely ineffective. During the first decade of the new century, attempts 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 such as "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. Technology and information businesses urged Congress to move cautiously in order not to foreclose innovative market responses.[28] Data brokers also worked assiduously to avoid meaningful FCRA oversight by exploiting the recursivity of the statute's definitional structure, representing that their products were just incomplete enough or anonymized enough or aggregated enough not to count as "consumer reports" and cautioning their subscribers not to use them that way.[29]

In the absence of a regulatory framework specifically tailored to the problems of surreptitious tracking and "behavioral advertising," the FTC attempted to fill the regulatory gap by asserting its general authority to police unfair and deceptive practices in commerce. As a practical matter, this meant that the construct of notice and consent became the dominant regulatory framework for evaluating online businesses' use of tracking techniques, and the "privacy policy"—a lengthy, turgid document disclosing information about an online entity's collection and processing of personal data—became the de facto vehicle for ensuring compliance.[30]

At the same time, the quest to track internet users by less transparent means continued, pushing ever more deeply into the logical and hardware layers of consumers' devices. Digital advertising companies ranging from emerging platform giants Google

and Facebook to new startup firms began developing techniques for identifying and tracking the MAC numbers that are permanently associated with all network-capable digital devices. As smart mobile platforms emerged and as additional techniques for device tracking and fingerprinting developed, tracking by both persistent, surreptitious cookies and permanent hardware identifiers became routine.[31] Telecommunications providers also got into the act. In 2014, 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; four years later, such revelations have come to seem ordinary.[32]

The Sensing Net

The radical expansion of surveillance capability via cookie technology was an unintended consequence of the search for a viable protocol for commercial transactions, but subsequent continuing extensions of surveillance capability 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 data collection has become a nearly continuous condition. Communications networks have been transformed into sensing networks, organized around always-on mobile devices and embedded, networked sensors that collect and transmit an astonishingly varied and highly granular stream of data about user behavior to powerful, interconnected platforms.

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 January 2017, the Pew Research Center reported that 77 percent of U.S. adults own a smartphone.[33] Even when used simply for one-to-one voice communications, mobile devices collect more kinds of data 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. And mobile application usage has grown exponentially. In January 2012, Apple's online App Store reported that downloads had reached 25 billion; by 2016, total downloads from the Apple, Android, Google, and Amazon online app stores exceeded 149 billion.[34]

In parallel with the increasingly widespread penetration of smart mobile devices and the continual expansion of those devices' capabilities, infrastructures for Web tracking have become complex and robust. In 2016, researchers attempting to catalog tracking techniques and map tracker networks uncovered a vast infrastructure, comprised of a heterogenous and continually evolving assortment of techniques, overlaid on a million of the Web's most popular sites. Dominant platform firms Google, Facebook, and Twitter maintain especially large networks, but a variety of other digital analytics firms also engage in pervasive and undisclosed device fingerprinting and tracking.[35]

Data harvested from people 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; 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 state actors.[36]

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 the legal rules enabling the ongoing construction of the sensing net are those relating to notice and consent, just as the FTC's enforcement practice has suggested. According to that way of reasoning about the collection and processing of personal data, data subjects have rights to control such activities but may exercise those rights by consenting 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. Even when users do have choices to prevent collection of certain types of data, the design of user interfaces, menu options, and accompanying disclosures systematically obscures those choices, guiding users instead toward options that involve more intensive data extraction.[37] And many important details about the kinds of behavioral data that the sensing net extracts simply are not disclosed to users at all. Within the sensing net, practices of data 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. 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.[38]

The conception of consent emerging from that default condition is unprecedented in the law of contracts or any other body of law. Consent to data extraction is being sublimated into the coded environment, and along the way it is being effectively redefined. In the contemporary networked marketplace, consent flows from status, not conduct, and 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 construction of the sensing net and the accompanying sublimation of consent work both to generate large quantities of data and to make public domain status the default condition for the data that are generated. Or, as data broker Acxiom (now rebranded as LiveRamp) puts it: "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."[39] Unlike land, which exists in finite quantity, data flows extracted from people are (in theory) subject to uncertainties: their 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 and 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 and productive appropriation.

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 data 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 data processing is global. The push to exploit the biopolitical public domain is a contest over a postcolonial terrain, in which global networked elites seek to harness the power of populations worldwide. 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 in 2013 had their origin in an asserted need to combat terrorist threats originating abroad. 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, and some Latin American countries have begun using electronic access cards and biometric technologies for policing and security purposes. A special strike force convened within the United States currently uses communications metadata to target drone strikes against suspected terrorist leaders.[40]

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 and deployment against vulnerable and minority populations. Both history and recent events suggest that those fears are well founded. Historian Alfred McCoy has documented the U.S. military's use of the Philippines as a test bed for surveillance techniques that subsequently migrated to the United States via the army's newly formed Military Intelligence Division during the years surrounding World War I.[41] In the post-9/11 environment, biometric identification first of noncitizens and subsequently of citizens has become an increasingly routine part of crossing the U.S. border; more recently, a number of state and local police departments have begun programs for biometric identification of suspects using facial recognition technologies trained on databases of driver license photographs.[42] Federal, state, and local law enforcement agencies have conducted prolonged, intrusive surveillance of Muslim and Latino communities, relying on a range of surveillance techniques including algorithmic analysis of communications metadata.[43] As Chapter 8 will discuss in more detail, a notable feature of these and other contemporary policing initiatives is the way they

incorporate participation by for-profit providers of surveillance data, techniques, and platforms.

In other global contexts, however, initiatives for personal data collection and processing are framed as development projects aimed at improving the living standards and prospects of the world's least fortunate peoples. In India, the Aadhaar 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.[44] Other initiatives attempt to use biometric and wireless technologies to compensate for the lack of developed financial and communications infrastructures. For example, in a number of African nations including Nigeria and South Africa, financial institutions 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.[45] In developing countries around the world, the Facebook Free Basics app supplies mobile handset users with curated lists of websites and services, including Facebook's own news feed. Use of those sites and services does not trigger data charges; meanwhile, Facebook collects comprehensive data about users and their activities.[46]

Among scholars and activists, a rich debate has unfolded about whether these initiatives and others like them should be understood as empowering or commodifying.[47] 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 impacts of such projects difficult to assess are worth considering carefully. Development of new surveillance infrastructures, such as those for the Aadhaar system, typically is contracted to multinational data processing companies. 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. As Chapter 1 described, new infrastructures for cashless payment also have deep connections to private finance capital. Facebook does not disclose information about its uses of data extracted via the Free Basics program at all. In addition, developing 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.[48]

The distinctive pattern of the postcolonial two-step also is visible in policing and social welfare initiatives directed at wholly domestic populations within the United States. Felony convicts are subject to mandatory DNA collection, and 28 states and the federal government require DNA collection from felony arrestees. In a decision 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.[49] But other biometric identification schemes already are in widespread use to identify recipients of government welfare programs, to conduct background checks of applicants for government jobs and security clearances, to monitor certain categories of temporary visa recipients, and in many other contexts involving vulnerable populations.[50] 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.[51]

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 adverse 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 presence or absence of certain other kinds of data (for example, unexplained gaps in debit or credit card purchase history) can obviate the need to ask. Platform differences also 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, and data collection via mobile devices is less transparent and less easily customized.[52] 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.

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.[53] The secrecy imperative overrides even official demands to produce information about data extraction practices and related agreements. In 2014, a Senate committee seeking to discover information about industry structure and contracting practices found itself effectively stonewalled as three of the nine largest data brokers in the country politely refused to answer questions about their data sources and their customers; the remaining six made voluminous submissions about their data sources and products but did not provide specific detail about their contract terms, their data processing techniques, or the extent to which they enforce policies assertedly put in place to protect consumers against abuse.[54] In enforcement proceedings before the FTC and in hearings before Congress, the dominant platform firms have pursued a strategy of deliberate obfuscation about the data flows that they collect, deflecting questions with vague and general responses and claiming inability to locate requested documents.[55]

In the context of the biopolitical public domain's productive logics, however, 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 constitute markets for personal data and information derived from it are acts of enclosure that complement the user-facing techniques explored in Chapter 1. They represent strategies for perfecting the appropriation of valuable resources from the (imagined) common.

In recent years, intellectual property scholars have invoked enclosure metaphorically to characterize legislative extensions of intellectual property rights, most notably copyright term extension intended to delay passage of copyrighted works into the public domain. So used, the term traces its origin to the Enclosure Movement in seventeenth century Britain, during which wealthy landholders erected physical fences to assert their control and ownership of common lands formerly used for grazing, hunting, and passage.[56] Inspired by that work, surveillance theorist Mark Andrejevic 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.[57]

But enclosure as a strategy also proceeds on a level that is more small-bore and ordinary than contemporary usage suggests. Information-related transactions routinely involve strategic uses of contractually-mandated secrecy. In particular, although intellectual property theory places "facts" permanently in the public domain, intellectual property practice traditionally has recognized a need for gap-filling protection in certain industries, and has looked to trade secrecy and contract law to fulfill that need. Participants in data-intensive industries, including both platforms and data brokers, routinely deploy trade secrecy law and contract to achieve a measure of exclusive control over the data that they collect. As we saw in Chapter 1, such practices of contractual enclosure are both strategic and performative: they simultaneously consummate processes of data appropriation and constitute those processes as lawful and foreordained.

Strategic uses of secrecy by platforms and data brokers also underscore the difference between public domain and commons as resource governance strategies. Governance as commons entails rules for maintaining a resource as open to community members. It also may involve rules imposing duties to use the resource sustainably and sanctions for abusing the privilege of membership.[58] Advocates for scientific and nonprofit research uses of collected personal data have sometimes argued (or have been happy to concede) that such collections should be governed as commons and that membership should be subject to various data protection obligations.[59] The public domain framing entails no comparable set of obligations; it functions and is intended to function as a backdrop for appropriation and private profit-seeking activity. Put differently, although the new information capitalists have worked hard to construct the sociotechnical conditions for the biopolitical public domain, they have not done this so all could share equally in its fruits. The race to harvest and profit from the public domain of personal data is intensely contested.

In short, the networks of secret agreements that characterize the emerging personal data industry, and that have frustrated observers seeking to map data flows and uses more precisely, 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. They represent strategies through which resources extracted from the biopolitical public domain are made to function as marketable assets and as sources of competitive advantage.

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 data also frames an approach to knowledge production that underwrites the processing of personal data 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 optimize both online and physical environments around desired patterns of attention and behavior. Data doubles are not marketed individually, but rather in groups with similar behavioral and risk characteristics; the participants in the data economy trade in people the way one might trade in commodity or currency futures. The new data refineries—and especially the dominant platforms that have reconstituted data markets around their own protocols for intermediation and legibility—infuse the data flows extracted from people with an epistemology optimized for surplus extraction. At the same time, they mark their operations and outputs with indicia of legal privilege. The public domain construct supports those processes from beginning to end.

Data Cultivars

In press releases, marketing materials, and other public statements, data brokers and platform firms frame the data harvested from individual users of networked information and communications technologies as raw streams of observation that are parsed, enhanced, and systematized through their own productive labor. Thus, for example, Acxiom (now LiveRamp) promises "meticulous data cleansing," while Oracle describes its "DaaS for Social" service as providing "categorization and enrichment of unstructured social and enterprise data." Less specifically but more famously, Google's self-proclaimed mission is "to organize the world's information and make it universally accessible and useful."[60]

In scholarly and policy communities, the "raw data" framing has generated considerable pushback. Scholars who study information systems argue that the "raw data" framing is not, and never could be, entirely accurate. Inevitably, data collection activities are structured by basic judgments about what to collect, what units of measurement to use, and what formats and metadata will be used to store and tag the data that are collected.[61] That is true of data gathered in disciplines far removed from personal data processing, such as geology and oceanography, and it is also true of data collected from and about people. For example, the decision to collect information about patterns of attention in automated gambling environments or patterns of "social reading" in platform environments, and to collect that information in a particular way, imposes a structure of sorts on the resulting data set.[62]

In theory, at least, the new, data-driven surveillance processes do differ importantly from earlier forms of commercial surveillance in terms of the way that flows of data are collected and processed. Scholars have long criticized the use of artificial categories to sort and segment populations of consumers, but new data mining techniques that emphasize pattern recognition and behavioral forecasting can move well beyond

predefined categories.[63] In addition, because such techniques can combine and synthesize heterogeneous data sets, an analyst looking for patterns is not constrained to search only in the ways for which any single data set is coded. Some legal scholars argue that the inherent dynamism of data mining for pattern recognition and prediction undercuts the traditional scholarly narrative of surveillance as imposing an artificial and often invidious discipline.[64]

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 may be formally agnostic about the content of a user's preferences—say, for burgers or sushi, for golf or bowling, for *Game of Thrones* or *ESPN College Football*, for scientifically vetted information about climate change projections or other narratives framing climate change as a conspiracy propagated by mainstream media and liberal elites—but it is not agnostic as to the kinds of information it collects and produces.

The technologies of the sensing net are designed to modulate surveillant attention, offering options tailored to what is known or inferred about data subjects' habits, beliefs, and inclinations. As social psychologist Shoshana Zuboff explains, that goal demands ever more detailed behavioral patterning. To achieve maximum accuracy and minimum uncertainty, the sensing net must plumb the depths of users' experiences, interpreting minute behavioral cues to ferret out underlying cognitive and emotional patterns.[65] To achieve maximum yield, the sensing net must keep users logged in and responsive to its harvesting mechanisms. As designers of mobile interfaces, social networking environments, and their embedded apps work to maximize behavioral data extraction, research on addiction pathways has become an explicit lodestar.[66]

Processes of data extraction within the sensing net are also and importantly participatory. Platform-based, massively-intermediated environments enable people seeking connection with each other to signal their affinities and inclinations using forms of shorthand—"Like", "Follow", "Retweet", and so on—that simultaneously enable data capture and extraction.[67] Sometimes, processes of technologically-intermediated signaling also call upon individual consumers to sort themselves into more definite categories by selecting various descriptors or categories—for example, "Professional", "Alumni", "Engaged", "Female Seeking Male", "Social Drinker"—informed by analysts' and marketers' sense of the types of patterns they are seeking.

Techniques for participatory data extraction are intended to cultivate habits of self-identification in a very particular way. In Scott Lash's formulation, these processes represent power becoming ontological: power expressed not through hegemonic control of meaning but rather through techniques for making the crowd known to itself.[68] They constitute the subjects of data-driven surveillance as knowing agents who attain freedom through a focused and purposeful—and often playful—consumerism that incorporates continual, automatic self-documentation. To the extent that self-sorting requires sets of choices within structured fields, it also effects a partial return to a more rigid patterning, undercutting the characterization of predictive analytics as protean and dynamic.

As these processes operate, they generate new informational byproducts that are themselves artifacts of the patterns with which their designers are concerned. The processes of harvesting and culling "raw" consumer personal data resemble 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, so the collection of personal data on an industrial scale inevitably adopts an active, curatorial stance regarding the items to be gathered.[69] 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.

Data Refineries

After personal data have been cultivated and harvested, they are processed to generate patterns and predictions about data subjects' preferences and behaviors. Like the data extraction and contracting practices discussed previously, the data processing practices of platform firms and data brokers also are shrouded in secrecy.[70] 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. Within the political economy of informational capitalism, sites for large-scale, automated processing of data flows extracted from people function as information-age refineries, converting those flows into the forms best suited for exploitation on an industrial scale.

Investigations of systems for automated, predictive processing of personal data through the lenses of privacy and data protection law typically have criticized such systems for offering artificial and instrumental forms of personalization based on externally determined logics. I have offered that characterization in my own work and have no quarrel with it. Modulation of surveillant attention is both a mode of privacy invasion and a mode of social control; it seeks "to produce tractable, predictable citizen-consumers whose preferred modes of both consumption and self-determination play out along predictable and profit-generating trajectories."[71] It therefore has profound implications both for individuals pursuing self-determination and for society more generally.

Even when scholarly critics of personal data processing focus on its larger social welfare implications, however, the view from privacy scholarship remains one that is both informed and limited by an individualistic frame of reference. Rights, including privacy and data protection rights, are tautologically individualistic, and scholarly preoccupation with the relationship between privacy and social shaping also testifies powerfully to anxiety about subjectivity's absence. The new data refineries, in contrast, operate on an entirely different scale. The agribusinesss model again supplies a useful analogy: the processing of data flows extracted from people within contemporary data refineries is comparable to the milling of corn and wheat to generate stable, uniform byproducts optimized for industrial food production.[72] Data refineries refine and massage flows of personal data to produce virtual representations—data doubles—optimized for modulating human behavior systematically.

Data doubles correlate to identifiable, flesh-and-blood human beings—they are sets of data that derive from and pertain to particular individuals and that can be used to

simulate individual behavior at a very high level of granularity—but their function within the emerging political economy of personal data is to subsume individual variation, idiosyncrasy, and self-awareness within a probabilistic and radically behaviorist gradient. Their purpose is to make human behaviors and revealed 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. (Despite glowing rhetoric about the promise of personalization in the digital era, we saw in Chapter 1 that this approach owes as much to Nielsen as it does to Page and Brin; the idea of analyzing current and target markets using demographic analysis reflects the influence of advertising models that are decades old.)

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.[73] Yet it has become 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. Data doubles afford a form of aggregated, population-based knowledge that enables participants in the political economy of informational capitalism to engage in "the management of fluctuating processes in an open field."[74] Indeed, in the era of ascendant neoliberal governmentality, it is data refineries' very privateness that gives their outputs normative and epistemological authority.[75]

Within the political economy of informational capitalism, the data refinery is a centrally important means of economic production. Its principal functions include not only knowledge production but also—and perhaps more importantly—data productivity. It promises new ways of making the data flows extracted from people economically productive within the framework of a capitalist political economy. That framing in turn suggests the importance of studying markets for the outputs of data refineries as markets—that is, as sites of economic exchange 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.[76] Those markets reflect extraordinary innovation of a sort, but they 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.

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. And it ignores entirely the question of supervening organizational logics imposed by the platforms within which data markets are increasingly embedded. 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 sociologists Michel Callon and Fabian Muniesa, that concise 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, the subject matter traded in markets must be conceived as a "calculable good": a good detached from its context in a way that enables it to be objectified, manipulated, and valued.[77] 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, barcode scanners, and coupons and the online system of a virtual "shopping cart," cookies for state management, and promotion codes or loyalty discounts both embed forms of calculative agency that enable the distributed 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 desirable.[78]

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.[79] Thus, for example, the procedures followed on the trading floor of the New York Stock Exchange, in Japanese tuna markets, and in the Amazon.com online marketplace each command unquestioned, deeply embedded assent as ways of ordering distribution and allocation.[80]

Although the terms and conditions of business-to-business transactions over the data refinery's inputs and outputs have proved astonishingly difficult to locate and bring into the light of day, the multi-billion-dollar trade in the byproducts of personal data processing speaks volumes about the emergence of each of these institutional components. To understand the processes by which calculable goods are defined in

markets served by the new data refineries, however, we must contend with two sets of complications, one hermeneutic and one organizational:

First, although it is customary in public-facing rhetoric about personal data collection and processing to refer to data subjects as individuals with singular wants and needs—and therefore to position them as the consumers whose desires are being served—that framing misdescribes the uses to which data doubles are put. The data-driven, predictive operations of the data refinery produce tranches of data doubles with probabilistically determined behavioral profiles. Businesses and other organizations of all sorts can then purchase different forms of access to those tranches as inputs (refined materials) to their own production processes.[81] Notably, Callon and Muniesa 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" goods for consumers, and often may do so by appealing to ideals of individualization.[82] Public-facing rhetoric about personal data harvesting and processing is most usefully understood in an analogous way, as an example of marketing-speak designed to encourage enrollment in the services that make up the sensing net (we will delve more deeply into such enrollment strategies in Chapter 3).

Behind the public-facing rhetoric about individualization and personalization, the data refinery's operators offer services that operate on populations. Generally speaking, those services advance two distinct but complementary types of profit-making strategies. One strategy identifies groups of high-value consumers as targets for surplus extraction by platform firms, data brokers, and their customers, including advertisers of all sorts but also employers, app developers, and others.[83] The other facilitates surplus extraction strategies optimized for riskier groups of consumers. For example, a principal cause of the 2008 financial crisis was risky subprime lending to high-risk buyers, and predatory lenders used tranches of data doubles to identify and target vulnerable populations.[84] As described in Chapter 1, the Dodd-Frank Act and implementing regulations established new, tighter standards for residential mortgage lending, but the use of data-driven predictive profiling to facilitate targeted risk-taking is gaining ground in other credit-related markets.[85] Together, strategies for targeting high-value and high-risk consumer pools offer powerful new formulas for market segmentation. Using the information supplied by the new data refineries, marketers can position their goods and services for target populations of consumers more effectively—and, in the process, can choose to target different offers to consumers with different profiles or to exclude consumers viewed as undesirable from viewing their offers at all.[86]

Second, the theory of markets as institutional structures for calculated exchanges predates the era of dominant information platforms, so it does not contend with the emergence of the platform as the core organizational logic of informational capitalism. As we saw in Chapter 1, platform-based, massively intermediated environments increasingly have colonized and rematerialized markets, placing themselves, their protocols for information exchange, their proprietary algorithms, and their massive computing resources at the center of a wide and growing variety of activities. Tellingly, major data brokers are now attempting to follow suit, rebranding themselves as platforms for specialized services—so, for example, LiveRamp (formerly Acxiom) now holds itself out as an "identity platform" for "powering the people-based marketing revolution."[87]

Platforms are data refineries given specific material and institutional form. The most dominant platforms enjoy direct access to vast populations of data subjects and have exploited that access to develop extractive relationships with seemingly limitless scope.

In sum, data markets are markets for calculated exchanges over tranches of data doubles derived probabilistically via behavioral patterning, and the calculable goods at the center of those exchanges are not the data doubles themselves but rather access to particular pools of data doubles constructed for particular purposes. The calculative agency required to power the exchanges consists of special-purpose frameworks for digital advertising, "customer relations management," "identity resolution," human resources management, and the like, and those frameworks increasingly are embedded in and structured by platform protocols.

Consuming Consumers

Scholarly investigations of techniques for processing personal data tend to frame the construction and manipulation of data doubles as knowledge production processes with secondary economic and legal-institutional implications, rather than as economic and legal-institutional processes with secondary knowledge production implications.[88] 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. It facilitates new and unprecedented surplus extraction strategies within which data flows extracted from people—and, by extension, people themselves—are commodity inputs, valuable only insofar as their choices and behaviors can be monetized.

The overriding goal of data refineries and data markets is not understanding but rather predictability in pursuit of profit. Data refineries are designed to offer powerful, high-speed techniques for matching populations with particular strategies 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, eliciting the patterns of behavior, content consumption, and content sharing already judged most likely to occur.[89] Such operations have a very particular economic purpose: They work to maintain and stabilize the available pool of consumer surplus so that it may be more reliably identified and easily extracted.

By virtue of their widening control over the sensing net's endpoints and the processes of data extraction and appropriation that occur there, the dominant platform-based purveyors of search, social networking, and connectivity enjoy correspondingly great control over the design and implementation of data-driven surplus extraction strategies. From the consumer perspective, the results of such processes in platform-based, massively intermediated environments may appear as reductions in search and transaction costs. Those strategies, however, have ripple effects on other market and social institutions, and indeed that is exactly their point. Both the material logics of data extraction and appropriation discussed earlier in this chapter and the epistemological logics of data cultivation and processing operate to submerge important exchange-related features of transactions and relationships in business-to-consumer markets. They produce

calculated exchanges that are increasingly etiolated and social processes that are increasingly colonized by privatized data flows.[90]

This description of the personal data economy, which posits users of networked information and communications technologies 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, or 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).[91] 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.

The *Moore* court, however, 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 byproduct. And, even as it took for granted the wisdom of granting patents on medical research byproducts, it worried fretfully about the costs to innovation of allowing proprietary claims to the raw materials used in medical research.[92] In short, the court's famous anti-commodification opinion articulated a powerful *logic of productive appropriation* that rendered Moore's asserted right to control the disposition of resources extracted from his body simply incoherent.

One can trace a similar elaboration of relative privilege and disentitlement in the evolving debates about data harvesting, processing, and use. Data brokers proudly tout their "unprecedented," "proprietary," and sometimes "patented" analytic techniques, while platform firms boast of their massive computing power and the cutting-edge algorithms that power their search engines, ad placement services, and news feeds.[93] Claims like those 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.[94] Other narratives about innovative exploitation of the biopolitical public domain locate romance in the technnologies themselves—in their power to find patterns, unlock new sources of competitive advantage, and enable new strategies for surplus extraction and accumulation—and that power is at its most romantic when its reach is most sweeping.[95] As we will see in Chapter 3, romantic narratives about data processing as innovation also do powerful normative work in political and regulatory arenas.

In short, there is more at stake here than a new model of knowledge production. The idea of a public domain of personal data alters the legal status of the inputs to and outputs of personal data processing. Its animating logic of productive appropriation is relational and distributive: it both suggests and legitimates a pattern of appropriation by some, with economic and political consequences for others.

The Power of Appropriative Privilege

The idea of a public domain of personal data sets in motion a familiar and powerful legal and economic just-so story. As it justifies the pervasive redesign of networked environments for data harvesting and positions the new data refineries and their outputs as sites of legal privilege, it naturalizes practices of appropriation by information platforms and data brokers. It subtly and durably reconfigures the legal and economic playing field, making effective regulation of its constituent activities more difficult to imagine.

One of the Hohfeldian framework's most important lessons is that legal privilege does not exist in a vacuum. It is always-already relative, entailing disempowerment on the part of someone else.[96] In the case of the biopolitical public domain, users of networked information and communications technologies have no right to contest the harvesting of their data, no right to fully informed participation in the proprietary knowledge production processes of the new data refineries, and no right to contest the preemptive superimposition of predictions derived from data doubles upon their activities, their social and emotional lives, and their aspirations.

For individuals and communities, the change in status from users and consumers to resources is foundational. The problem is not simply that the biopolitical public domain facilitates commodification (though it does) or that it enables discrimination (though it does that too), but more fundamentally that it subordinates considerations of human well-being and human self-determination to the priorities and values of powerful economic actors. 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 economic transactions. The emerging system of data-driven predictive profiling is designed to strip away opportunities for bargaining and arbitrage, 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 ability" while goods and services flow "to each according to his [manufactured] needs."[97]

The systemic implications of pervasive data harvesting and predictive profiling are equally profound. Reimagining consumer markets as sites of unilateral technosocial sorting undermines both their utility as markets and their legitimacy as decentralized governance processes. At least according to theory, in a capitalist society, market transactions function as an essential mode of governance. The conception of the biopolitical public domain expressed by the commercial surveillance economy is a hierarchical conception that sits in fundamental tension with the market-libertarian ideal. Despite the popularity of transactional consent as a frame for neoliberal policy discourse, the surveillance economy leaves consent—and, for that matter, volition—with very little work to do.

As we are about to see next, the sensing net and the data refinery have also catalyzed systemic changes in the operation of networked digital media ecologies.. Those

changes too have inspired new forms of legal-institutional entrepreneurship by the actors that they benefit.

---

[1] Jessica Litman, "The Public Domain," *Emory Law Journal* 39 no. 4 (1990): 965-1023; Anupam Chander & Madhavi Sunder, "The Romance of the Public Domain," *California Law Review*, 92 no. 5 (2004): 1331-1373.
[2] Within the U.S. legal system, the definitive treatment of these questions is Johnson v. M'Intosh, 21 U.S. 543 (1823).
[3] David Feller, *The Public Lands in Jacksonian Politics* (Madison: University of Wisconsin Press, 1984); Paul W. Gates, *The Jeffersonian Dream: Studies in the History of American Land Policy and Development* (Albuquerque: University of New Mexico Press, 1996).
[4] John Locke, *Second Treatise of Government*, ed. C.B. Macpherson (Indianapolis: Hackett, 1980), 29.
[5] Chander & Sunder, "The Romance of the Public Domain."
[6] "Welcome to the People Connect Family of Products," Intelius, https://perma.cc/H5EK-4HZD (last visited June 24, 2018); "Get Data on 80% of Your Customers," Towerdata, https://perma.cc/9JTC-S2WS (last visited June 24, 2018); "Powering the Global Real Estate Economy," CoreLogic, https://perma.cc/K2X7-8YGD (last visited June 24, 2018); "The Only Universal Threat Intelligence Solution," Recorded Future, https://perma.cc/5YXW-J2RB (last visited June 24, 2018).
[7] Hearing before the Senate Committee on Commerce, Science, and Transportation, "What Information Do Data Brokers Have on Consumers, and How Do They Use It?", 113 Cong., 1st Sess. (Dec. 18, 2013) (statement of Tony Hadley, Senior Vice President of Government Affairs and Public Policy, Experian).
[8] Hal R. Varian, "Beyond Big Data," *Business Economics*, 49 no. 1 (2014): 27-31, 29.
[9] U.S. Senate Committee on Commerce, Science, and Transportation, Office of Oversight and Investigations Majority Staff, "A Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes" (Dec. 18, 2013), https://perma.cc/SEC4-GEGB. Other useful overviews of the data broker industry include Upturn, "Data Brokers in an Open Society" (Nov. 2016), https://perma.cc/AL2X-SUEM; U.S. Federal Trade Commission, "Data Brokers: A Call for Transparency and Accountability" (May 2014), https://perma.cc/K6FK-TJGA.
[10] On the new legislation and the abuses that had prompted it, see Robert M. McNamara, Jr., "The Fair Credit Reporting Act: A Legislative Overview," *Journal of Public Law* 22 no. 1 (1973): 67-101.
[11] See, for example, Hearings before Subcomm. on Consumer Affairs of the House Comm. on Banking and Currency on H.R. 16340, 91st Cong., 2d Sess. 108 (1970) (testimony of John L. Spafford, President, Associated Credit Bureaus Inc.). A useful summary of the legislative history on this point is National Consumer Law Center, *Fair Credit Reporting Act* 3rd ed., §1.4.3 (Boston: National Consumer Law Center, 1994).
[12] Fair Credit Reporting Act, 15 U.S.C. §1681a(d)(1), (f) (2018) .
[13] Pauline T. Kim & Erik A. Hanson, "People Analytics and the Regulation of Information under the Fair Credit Reporting Act," *St. Louis University Law Journal* 61 no. 1 (2016): 17-34.
[14] Oscar H. Gandy, Jr., *The Panoptic Sort: A Political Economy of Personal Information*. (Boulder, Colo: Westview, 1993); see also Robert D. Manning, *Credit Card Nation: The Consequences of America's Addiction to Credit* (New York: Basic Books, 2000), 106-24.
[15] For a good explanation, see David M. Kristol, "HTTP Cookies: Standards, Privacy, and Politics," *ACM Transactions on Internet Technology*, 1 no. 2 (2001): 152-56.
[16] U.S. Patent 5,774,670, "Persistent Client State in a Hypertext Transfer Protocol Based Client-Server System"; Kristol, "HTTP Cookies," 159.
[17] Tim Jackson, "This Bug in Your PC Is a Smart Cookie," *Financial Times* (Feb. 12, 1996), 15; Lee Gomes, "Web 'Cookies' May Be Spying on You," *San Jose Mercury News* (Feb. 13, 1996), 1C.
[18] U.S. Federal Trade Comm'n, Public Workshop on Consumer Privacy in the Global Information Infrastructure, June 4-5, 1996, https://perma.cc/FSL4-SB7J.
[19] Richard M. Smith, "The Web Bug FAQ" (Nov. 11, 1999), https://perma.cc/5HVY-FW6E.
[20] Kristol, "HTTP Cookies."

[21] On the evolution of massively multiplayer and social gaming, see Simon Egenfeldt-Nielsen, Jonas Heide Smith, & Susana Pajares Tosca, *Understanding Video Games: The Essential Introduction*, 3rd ed. (New York: Routledge, 2016), 108-113; Lauren Indvik, "The Fascinating History of Online Role-Playing Games," Mashable (Nov. 14, 2012), https://perma.cc/F68U-NHSN; Riad Chikhani, "The History of Gaming: An Evolving Community," *Tech Crunch* (Oct. 31, 2015), https://perma.cc/GRK3-SL7Y.
[22] Rebecca Buckman, "Investors to Web Start-Ups: Where's the Advertising?," *Wall Street Journal* (Aug. 21, 2007), archived at CommercialAlert.org, https://perma.cc/V4WG-RMMU; see also Rebecca Greenfield, "2012: The Year Facebook Finally Tried to Make Some Money," *The Atlantic* (Dec. 14, 2012), http://perma.cc/DS6B-U7H9.
[23] Steven Levy, *In the Plex: How Google Thinks, Works, and Shapes Our Lives* (New York: Simon & Schuster, 2011), 87-120; Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (New York: Polity, 2019), 71-85.
[24] David Kirkpatrick, *The Facebook Effect: The Inside Story of the Company that Is Connecting the World* (New York: Simon & Schuster, 2010), 218-63.
[25] Leanne Roderick, "Discipline and Power in the Digital Age: The Case of the U.S. Consumer Data Broker Industry," *Critical Sociology* 40 no. 5 (2014): 739; Chris Jay Hoofnagle, "Big Brother's Little Helpers: How ChoicePoint and Other Commercial Data Brokers Collect and Package Your Data for Law Enforcement," *North Carolina Journal of International Law and Commercial Regulation* 29 no. 4 (2004): 595-638.
[26] "List of Mergers and Acquisitions by Alphabet," Wikipedia, https://perma.cc/8TKN-F3B8 (last visited Dec. 13, 2018); "List of Mergers and Acquisitions by Facebook," Wikipedia, https://perma.cc/YR76-RNDS (last visited Dec. 13, 2018).
[27] McKinsey Global Institute, "Big Data: The Next Frontier for Innovation, Competition, and Productivity" (May 2011), https://perma.cc/C8X8-Q3SX; Jeff Kelly, "Big Data: Hadoop, Business Analytics and Beyond," Wikibon (Feb. 5, 2014), https://perma.cc/8U2W-RWAV.
[28] 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. (Jan. 26, 2005), 17-14 (statement of Ira Rubinstein, Associate General Counsel, Microsoft Corporation).
[29] Sarah Jeong, "You Can't Escape Data Surveillance in America," *The Atlantic* (April 29, 2016), https://perma.cc/Q4BM-CL98; Astra Taylor & Jathan Sadowski, "How Companies Turn Your Facebook Activity Into a Credit Score," *The Nation* (May 27, 2015), https://perma.cc/2RF9-J55W; Opinion, Julie Brill, "Demanding Transparency from Data Brokers," *Washington Post* (Aug. 15, 2013), https://perma.cc/2X95-G4GM.
[30] Chris Jay Hoofnagle, *Federal Trade Commission Privacy Law and Policy* (New York: Cambridge University Press, 2016), 145-192. As Hoofnagle explains, the FTC also learned over time to draw on elements from its false advertising toolkit in policing companies' disclosures and interface designs.
[31] Steven Englehardt & Arvind Narayanan, "Online Tracking: A 1-Million-Site Measurement and Analysis," in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security* (New York: ACM, 2016), 1388-1401; Jeremy Gillula & Seth Schoen, "An Umbrella in a Hurricane: Apple Limits Mobile Device Location Tracking," EFF Deeplinks (June 11, 2014), https://perma.cc/2M85-BY2T.
[32] Brian X. Chen & Natasha Singer, "Verizon Wireless to Allow Complete Opt-Out of Mobile 'Supercookies,'" *New York Times Online* (Jan. 30, 2015), https://perma.cc/XYR5-6DVC; Jon Brodkin, "AT&T Buying Company that Delivers Targeted Ads Based on Your Web Browsing," *Ars Technica* (June 25, 2018), https://perma.cc/AEF3-555C; Karl Bode, "Another Day, Another Massive Cellular Location Data Privacy Scandal We'll Probably Do Nothing About," *TechDirt* (Jan. 9, 2019), https://perma.cc/2FQX-X83T.
[33] Aaron Smith, "Record Shares of Americans Now Own Smartphones, Have Home Broadband," Pew Research Center (Jan. 12, 2017), https://perma.cc/ZLQ3-ZBV2.
[34] Lex Friedman, "The App Store Turns Five: A Look Back and Forward," *Macworld* (July 8, 2013), https://perma.cc/5TKN-EFSW; Arytom Dogtiev, "App Download and Usage Statistics 2017," Business of Apps (Oct. 16, 2017), https://perma.cc/W2X8-2UJ5.

[35] Englehardt & Narayanan, "Online Tracking"; Timothy Libert, "Exposing the Hidden Web: An Analysis of Third-Party HTTP Requests on One Million Websites," *International Journal of Communication* 9 (2015): 3544-3561; see also Ibrahim Altaweel, Nathaniel Good, & Chris Jay Hoofnagle, "Web Privacy Census," *Technology Science* (Dec. 15, 2015), https://perma.cc/H8WV-7T63; Kashmir Hill, "I Cut the 'Big Five' Tech Giants from My Life. It Was Hell," *Gizmodo* (Feb. 7, 2019), https://perma.cc/8HP4-9AFV.
[36] For different perspectives on these developments, see McKinsey Global Institute, "The Internet of Things: Mapping the Value Beyond the Hype" (June 2015), https://perma.cc/34UX-AJYX; Mark Andrejevic & Mark Burdon, "Defining the Sensor Society," *Television and New Media* 16 no. 1 (2015); 19-36; Kelly A. Gates, *Our Biometric Future: Facial Recognition Technology and the Culture of Surveillance* (New York: New York University Press, 2011).
[37] On the manipulability of consent, see Alessandro Acquisti, Laura E. Brandimarte, & George Loewenstein, "Privacy and Human Behavior in the Age of Information," *Science* 347 (2015): 509-14; Woodrow Hartzog, *Privacy's Blueprint: The Battle to Control the Design of New Technologies* (Cambridge, Mass.: Harvard University Press, 2018), 21-55; Lauren E. Willis, "When Nudges Fail: Slippery Defaults," *University of Chicago Law Review*, 80 no. 3 (2013): 1170–1200.
[38] Mireille Hildebrandt & Antoinette Rouvroy, eds., *Law, Human Agency and Autonomic Computing* (New York: Routledge, 2011); Julie E. Cohen, *Configuring the Networked Self: Law, Code, and the Play of Everyday Practice* (New Haven: Yale University Press, 2012), 200-01; Jeffrey O. Kephart & David M. Chess, "The Vision of Autonomic Computing," *Computer* 36 no. 1 (2003): 41-50. On the sensing net as a mechanism for "passiv-izing" interactivity, see Andrejevic & Burdon, "Defining the Sensor Society."
[39] Kamal Tahir, "Marketing in the Internet of Things (IoT) Era," Acxiom Perspectives (Apr. 9, 2015), https://perma.cc/2ZK9-UDM4.
[40] On military uses of biometric technologies, see for example Tanya Polk, "Handheld Device Helps Soldiers Detect the Enemy," U.S. Army (Jan. 14, 2010); https://perma.cc/25VX-KCSG; George I. Seffers, "U.S. Defense Department Expands Biometrics Technologies, Information Sharing," *SIGNAL Magazine* (Oct 2010). On biometric surveillance and policing in Latin America, see Nelson Arteaga Botello, "Surveillance and Urban Violence in Latin America," in *Routledge Handbook of Surveillance Studies*, eds. Kirstie Ball, Kevin D. Haggerty & David Lyon, (New York: Routledge, 2012), 259-66. On targeted drone strikes, see Jeremy Scahill & Glenn Greenwald, "The NSA's Secret Role in the U.S. Assassination Program," *The Intercept* (Feb. 10, 2014), https://perma.cc/8ZFR-EC22; David Cole, "'We Kill People Based on Metadata,'" *New York Review of Books* (May 10, 2014), https://perma.cc/ERY2-Z44L.
[41] Alfred McCoy, *Policing America's Empire: The United States, the Philippines, and the Rise of the Surveillance State* (Madison: University of Wisconsin Press, 2009).
[42] Gates, *Our Biometric Future*; Clare Garvie, Alvaro Bedoya, & Jonathan Frankle, "The Perpetual Lineup: Unregulated Police Face Recognition in America," Center on Privacy and Technology, Georgetown Law (Oct. 18, 2016), http://perma.cc/DM3U-ZPYD; Harrison Rudolph, Laura M. Moy, & Alvaro N. Bedoya, "Not Ready for Takeoff: Face Scans at Airport Departure Gates," Center on Privacy & Technology, Georgetown Law (Dec. 21, 2017), http://perma.cc/V288-MCM4.
[43] Matt Apuzzo & Joseph Goldstein, "NYPD Drops Unit that Spied on Muslims," *New York Times* (Apr. 16, 2014), A1, https://perma.cc/C7EC-489Q; Diala Shamas, "Where's the Outrage when the FBI Targets Muslims?", *The Nation* (Oct. 31, 2013), https://perma.cc/Q8DY-JAK8; Glenn Greenwald & Murtaza Hussein, "Meet the Muslim-American Leaders the FBI and NSA Have Been Spying On," *The Intercept* (July 9, 2014), https://perma.cc/HMC9-43BC; Adam Schwartz, "No Hunting Undocumented Immigrants with Stingrays," Electronic Frontier Foundation (May 19, 2017), http://perma.cc/YN63-6GRD.
[44] Vjiay Sathe, "The World's Most Ambitious ID Project," *Innovations*, 6 no. 2 (2011): 39-65; Manan Kakkar, "Companies, Processes and Technology behind India's UID Project, Aadhaar" (Oct. 1, 2010), https://perma.cc/96U3-CQBL; Glyn Moody, "Aadhaar – Soon, in India, Everyone *Will* Be a Number," *TechDirt* (July 7, 2015), https://perma.cc/2UKV-V6Z6.
[45] "Press Release: MasterCard, MasterCard-branded National eID Card Launched in Nigeria," MasterCard (Aug. 28, 2014), at https://perma.cc/A5XF-FETC; Adam Oxford, "Nigeria Launches New Biometric ID Card – Brought to you by MasterCard," ZDNet (Aug. 29, 2014), https://perma.cc/9U3X-ZMUT; "SA Banks Begin Fingerprint Verification," South Africa: The Good News (Nov. 9, 2011), http://perma.cc/6FAA-23SR.

[46] Advox, "Can Facebook Connect the Next Billion?," Global Voices (July 27, 2017), https://perma.cc/U9QR-8NTA.
[47] See, for example, Amiya Bhatia & Jacqueline Bhabha, "India's Aadhaar Scheme and the Promise of Inclusive Social Protection," *Oxford Development Studies* 45 no. 1 (2017): 64-79; Shweta Punj, "A Number of Changes," *Business Today* (Mar. 4, 2012), https://perma.cc/LY3S-9Z86; Jean Dreze, "Unique Identity Dilemma," *The Indian Express* (Mar. 19, 2015), https://perma.cc/L4DB-9CYK; Manish Singh, "India's Database with Biometric Details of its Billion Citizens Ignites Privacy Debate," Mashable (Feb. 13, 2017), https://perma.cc/4W4F-WQ78; P. Arun, "Uncertainty and Insecurity in Privacyless India: A Despotic Push towards Digitalization," *Surveillance and Society* 15 nos. 3/4 (2017): 456-464.
[48] On the contracting of data infrastructure development to multinationals, see Linnet Taylor & Dennis Broeders, "In the Name of Development: Power, Profit and the Datafication of the Global South," *Geoforum* 64 (2015): 229-237. On the challenges of implementing data protection in developing countries, see Linnet Taylor, "Data Subjects or Data Citizens? Addressing the Global Regulatory Challenge of Big Data," in *Freedom and Property of Information: The Philosophy of Law Meets the Philosophy of Technology*, eds. Mireille Hildebrandt & Bibi van den Berg (New York: Routledge, 2016), 81-105. On free flow provisions in trade agreements, see Chapter 7, pp. 215-16, 223-24.
[49] Maryland v. King, 569 U.S. 1958 (2013).
[50] On the uses and implications of biometric identification techniques, see Gates, *Our Biometric Future*, 54-58; Michele Estrin Gilman, "The Class Differential in Privacy Law," *Brooklyn Law Review.* 77 no. 4 (2012): 1389-1445; Torin Monahan, ed., *Surveillance and Security: Technological Politics and Power in Everyday Life* (New York: Routledge, 2006).
[51] U.S. Department of Education, Data.Ed.Gov, https://perma.cc/2CDB-8FYY (last visited Apr. 11, 2019); U.S. Department of Health & Human Services, HealthData.gov, https://perma.cc/QH8J-6GTU (last visited Apr. 11, 2019).
[52] Pew Research Center, "The Smartphone Difference" (April 2015), 16-19, https://perma.cc/KN9V-53EE.
[53] For a comprehensive exploration, see Frank Pasquale, *The Black Box Society: The Secret Algorithms that Control Money and Information* (Cambridge, Mass.: Harvard University Press, 2015).
[54] Senate Committee on Commerce, Science, and Transportation, "A Review of the Data Broker Industry," 10-11. See also Federal Trade Commission, "Data Brokers," 7-10 (describing results of a similar survey of a list of companies that partially overlapped the Senate committee's list).
[55] Zuboff, *The Age of Surveillance Capitalism*, 145-48, 159-61; "Transcript of Mark Zuckerberg's Senate Hearing," *Washington Post* (April 10, 2018), https://perma.cc/2UQ5-CWYD; "Transcript of Zuckerberg's Appearance before House Committee," *Washington Post* (Apr. 11, 2018), https://perma.cc/LSZ7-4ECA.
[56] Yochai Benkler, "Free as the Air to Common Use: First Amendment Constraints on Enclosure of the Public Domain," *New York University Law Review* 74 no. 2 (1999): 363; James Boyle, "The Second Enclosure Movement and the Construction of the Public Domain," *Law and Contemporary Problems* 66 nos. 1-2 (1998): 33-40.
[57] Mark Andrejevic, *iSpy: Surveillance and Power in the Interactive Era* (Lawrence: University Press of Kansas, 2007) 2-4, 104-11.
[58] See Yochai Benkler, *The Wealth of Networks: How Social Production Transforms Markets and Freedom* (New Haven: Yale University Press, 2006), 60-61; Brett M. Frischmann, *Infrastructure: The Social Value of Shared Resources*, (New York: Oxford University Press, 2012), 7-9, 91-95.
[59] See, for example, Frederik Zuiderveen Borgesius, Jonathan Gray, & Mireille van Eechoud, "Open Data, Privacy, and Fair Information Principles: Towards a Balancing Framework," *Berkeley Technology Law Journal* 30 no. 3 (2015): 2073, 2098-2101; Arthur W. Toga & Ivo V. Dinov, *Sharing Big Biomedical Data*, *Journal of Big Data* 2 (2015): 7, doi:10.1186/s40537-015-0016-1; Jane Yakowitz, "Tragedy of the Data Commons," *Harvard Journal of Law and Technology* 25 no. 1 (2011): 1, 42-50.
[60] Acxiom, "Data Solutions," http://perma.cc/6AW3-7CWE; Oracle, Press Release, "New Oracle Data Cloud and Data-as-Service Offerings Redefine Data-Driven Enterprise" (July 22, 2014), http://perma.cc/V25M-8EHK; "About," Google AI (last visited Dec. 14, 2018), https://perma.cc/6XXX-UXZH.
[61] danah boyd & Kate Crawford, "Critical Questions for Big Data: Provocations for a Cultural, Technological, and Scholarly Phenomenon," *Information, Communication & Society* 15 no. 5 (2012): 662-679; Lisa Gitelman, ed., "*Raw Data" Is an Oxymoron*, (Cambridge, Mass: MIT Press, 2013).

[62] Natasha Dow Schull, *Addiction by Design: Machine Gambling in Las Vegas* (Princeton: Princeton University Press, 2012); Neil M. Richards, "The Perils of Social Reading," *Georgetown Law Journal*, 101 no. 3 (2013): 689-724.
[63] A leading critique of traditional, profile-based market segmentation is Gandy, *The Panoptic Sort*.
[64] See, for example, Mark MacCarthy, "In Defense of Big Data Analytics," in *The Cambridge Handbook of Consumer Privacy*, eds. Evan Selinger, Jules Polonetsky, & Omer Tene (New York: Cambridge University Press, 2018), 47-78; Tal Zarsky, "Automated Prediction: Perception, Law, and Policy," *Communications of the ACM*, 55 no. 9 (2012): 33-35; Tal Zarsky, "Transparent Predictions," *University of Illinois Law Review*, 2013 no. 4 (2013) 1527-28.
[65] Zuboff, *The Age of Surveillance Capitalism*, 270-90; see also Kirstie Ball, "Exposure: Exploring the Subject of Surveillance," *Information, Communication and Society* 12 no. 5 (2009): 639-57. On surveillance as modulation, see John Cheney-Lippold, "A New Algorithmic Identity: Soft Biopolitics and the Modulation of Control," *Theory, Culture and Society* 28 no. 6 (2011): 164-181; Julie E. Cohen, "What Privacy Is For," *Harvard Law Review*, 126 no. 7 (2013): 1915-1918; Greg Elmer, *Profiling Machines: Mapping the Personal Information Economy* (Cambridge, Mass.: MIT Press, 2004), 41-50.
[66] Bianca Bosker, "The Binge Breaker," *The Atlantic* (Nov. 2016), https://perma.cc/P7UJ-DEVD; Tristan Harris, "How Technology Is Hijacking Your Mind—from a Magician and Google Design Ethicist," *Thrive Global* (May 18, 2016), https://perma.cc/WG2Z-TLWJ; Adam Alter, *Irresistible: The Rise of Addictive Technology and the Business of Keeping Us Hooked* (University Park, Pa.: Penn State University Press, 2017). On design for addiction more generally, see Schull, *Addiction by Design*.
[67] Jose van Dijck, *The Culture of Connectivity: A Critical History of Social Media* (New York: Oxford University Press, 2013), 46-65; Zuboff, *The Age of Surveillance Capitalism*, 457-61.
[68] Scott Lash, "Power after Hegemony: Cultural Studies in Mutation?," *Theory, Culture & Society* 24 no. 3 (2007): 55-78; see also Cheney-Lippold, "A New Algorithmic Identity."
[69] Michael Pollan, *The Omnivore's Dilemma: A Natural History of Four Meals* (New York: Penguin, 2007), 30-31, 36-37, 41-42, 45, 58-59.
[70] Pasquale, *The Black Box Society*, 22-42, 64-80. As Zuboff explains, the secrecy imperative flows from the radical behaviorist premises underlying data-driven profiling; according to those premises, awareness that one's reactions and behaviors are being tracked is "the enemy" because it introduces confounding behavioral signals. Zuboff, *The Age of Surveillance Capitalism*, 88-89, 306-08.
[71] Cohen, "What Privacy Is For," 1917.
[72] Pollan, *The Omnivore's Dilemma*, 17-19, 85-99.
[73] On biopower, biopolitics, and their relation to state power, see Michel Foucault, *The History of Sexuality, vol. 1: An Introduction,* trans. Robert Hurley (New York: Random House, 1978); see also, for example, Catherine Mills, "Biopolitics and the Concept of Life," in *Biopower: Foucault and Beyond*, eds. Vernon W. Cisney & Nicolae Morar (Chicago: University of Chicago Press, 2016), 82-101.
[74] Thomas Nail, "Biopower and Control," in *Between Deleuze and Foucault*, eds. Nicolae Morar, Thomas Nail & Daniel W. Smith (Edinburgh: University of Edinburgh Press, 2016), 259; see also Cheney-Lippold, "A New Algorithmic Identity"; Frederic Gros, "Is There a Biopolitical Subject? Foucault and the Birth of Biopolitics," in *Biopower: Foucault and Beyond*, 259-73.
[75] On neoliberal governmentality and its emphasis on the primacy of markets, see the Introduction, pp. 6-7.
[76] Pollan, *The Omnivore's Dilemma,* 17-19, 73-79, 85-99.
[77] Michel Callon & Fabian Muniesa, "Peripheral Vision: Markets as Calculative Collective Devices," *Organization Studies* 26 no. 8 (2005): 1229-50, 1232-36.
[78] Callon & Muniesa, "Peripheral Vision," 1236-39.
[79] Callon & Muniesa, "Peripheral Vision," 1239-43.
[80] On the tuna market, see Eric A. Feldman, "The Tuna Court: Law and Norms in the World's Premier Fish Market," *California Law Review* 94 no. 2 (2006): 313-69.
[81] On the representation of consumers as resources to be accounted for, see Greg Elmer, "IPO 2.0: The Panopticon Goes Public," *Media Tropes*, 4 no. 1 (2013): 1-16; Mireille Hildebrandt, *Smart Technologies and the End(s) of Law* (Northampton, Mass.: Edward Elgar, 2015), 91-93.
[82] Callon & Muniesa, "Peripheral Vision," 1235-36.
[83] For examples of some of the categories into which high-value consumers are sorted, see U.S. Senate Committee on Commerce, Science, and Transportation, Office of Oversight and Investigations Majority

Staff, "A Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes" (Dec. 18, 2013), 24.

[84] On the economic appeal of high-risk pools and the use of numerical credit scoring to construct such pools in the mortgage finance context, see Martha Poon, "From New Deal Institutions to Capital Markets: Commercial Consumer Risk Scores and the Making of Subprime Mortgage Finance," *Accounting, Organizations, and Society* 34 no. 5 (2009): 654-674. For other explorations of practices targeting vulnerable populations, see Virginia Eubanks, *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor* (New York: St. Martin's Press, 2018); Seeta Pena Gangadharan, "Digital Inclusion and Data Profiling," *First Monday* 17 no. 5 (2012): 7, https://doi.org/10.5210/fm.v17i5.3821; Nathan Newman, "The Costs of Lost Privacy: Consumer Harm and Rising Economic Inequality in the Age of Google," *William Mitchell Law Review* 40 no. 2 (2014): 876-82; Safiya Umoja Noble, *Algorithms of Oppression: How Search Engines Reinforce Racism* (New York: New York University Press, 2018); see also Senate Committee on Commerce, Science, and Transportation, "A Review of the Data Broker Industry," 24-27; Federal Trade Commission, "Data Brokers," 19-25.

[85] On the rise of "behavioral credit scoring," see Robinson + Yu, "Knowing the Score: New Data, Underwriting, and Marketing in the Consumer Credit Marketplace" (Oct. 2014), https://perma.cc/7V2P-4J2A; Mikella Hurley & Julius Adebayo, "Credit Scoring in the Era of Big Data," *Yale Journal of Law and Technology* 18 (2016): 148-216.

[86] On exclusion, see Julia Angwin, Ariana Tobin, and Madeleine Varner, "Facebook is (Still) Letting Housing Advertisers Exclude Users by Race," *ProPublica* (Nov. 21, 2017), http://perma.cc/9K9C-JE6K; April Glaser, "Facebook Is Eliminating the Easiest Ways to Commit Housing and Employment Discrimination—but Not All the Ways," *Slate* (Mar. 20, 2019), https://perma.cc/JRL4-NKGK. On differential promotion and pricing, see Greg Petro, "Dynamic Pricing: Which Customers Are Worth The Most? Amazon, Delta Airlines And Staples Weigh In," *Forbes Online* (Apr. 17, 2015), https://perma.cc/RT63-MYDU; Jennifer Valentino-Devries, Jeremy Singer-Vine & Ashkan Soltani, "Websites Vary Prices, Deals Based on Users' Information," *Wall Street Journal* (Dec. 24, 2012), https://perma.cc/HJ2V-PY3Y; Olga Kharif, "Supermarkets Offer Personalized Pricing," *Bloomberg News* (Nov. 15, 2013), https://perma.cc/BT6X-K963; Dana Mattioli, "On Orbitz, Mac Users Steered to Pricier Hotels," *Wall Street Journal* (Aug. 23, 2012), https://perma.cc/UQK9-XBGR; "Flexible Figures," *The Economist* (Jan. 30, 2016), https://perma.cc/9WZ2-C6CS; Carlo Longino, "SF Giants Test Dynamic Ticket Pricing," *TechDirt* (May 20, 2009), https://perma.cc/L99T-KUMS; Mike Masnick, "Citizen Journalism Bites into Amazon's Attempts at Dynamic Pricing," *TechDirt* (Jan. 4, 2007), https://perma.cc/K5MW-Q72C.

[87] See "About LiveRamp," LiveRamp, https://perma.cc/5LVM-VU62 (last visited April 6, 2019).

[88] An important early exception identifying Big Data as an expression of a logic of economic accumulation, was Shoshana Zuboff, "Big Other: Surveillance Capitalism and the Prospects of an Information Civilization," *Journal of Information Technology*, 30 no. 1 (2015): 75-89.

[89] This terminology combines the concept of the nudge, imported from behavioral economics and now widely used by both critics and admirers of data-based analytics, with that of preemption as used by Hildebrandt, *Smart Technologies and the End(s) of Law*, 57-61, and Ian Kerr & Jessica Earle, "Prediction, Preemption, Presumption: How Big Data Threatens Big Picture Privacy," *Stanford Law Review Online*, 66 (2013): 65-72 68-70. The preemptive nudge simultaneously suggests and forecloses. See also Karen Yeung, "'Hypernudge': Big Data as a Mode of Regulation by Design," *Information, Communication, and Society* 20 no. 1 (2017): 118-126.

[90] On data appropriation as a new iteration of the historic and political logics of colonialism, see Nick Couldry & Ulises A. Mejias, "Data Colonialism: Rethinking Big Data's Relation to the Contemporary Subject," *Television and New Media* (Sept. 2, 2018), https://doi.org/10.1177/1527476418796632.

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

[92] For discussion of these points, see James Boyle, *Shamans, Software, and Spleens: Law and the Construction of the Information Society*, (Cambridge, Mass: Harvard University Press, 1998), 106-07.

[93] "New Oracle Data Cloud and Data-as-Service Offerings Redefine Data-Driven Enterprise," Oracle (July 22, 2014), https://perma.cc/E6AR-4XH3 (unprecedented intelligence"); Spokeo, "About," https://perma.cc/L78B-RZX6 (last visited June 24, 2018) ("proprietary merge technology"); Intelius, "Products," https://perma.cc/H5EK-4HZD (last visited June 24, 2018) ("proprietary technology"); ID

Analytics, "Company Overview," https://perma.cc/9PF7-ESSN (last visited June 24, 2018) ("patented analytics").

[94] Boyle, *Shamans, Software, and Spleens*, 108-43; Chander & Sunder, "The Romance of the Public Domain," 1339-40.

[95] For discussion of this point, see Cohen, "What Privacy Is For," 1921-23.

[96] Wesley Newcomb Hohfeld, "Some Fundamental Legal Conceptions as Applied in Judicial Reasoning," *Yale Law Journal* 23 no. 1 (1913): 32-44.

[97] Cf. Karl Marx, "Critique of the Gotha Program," in *Marx: Later Political Writings*, ed. & trans. Terrell Carver (New York: Cambridge University Press, 1996), 208-226; see also Marion Fourcade & Kieran Healy, "Seeing Like a Market." *Socio-Economic Review* 15 no. 1 (2017): 9-29.