Marion Fourcade, UC Berkeley
Jeffrey Gordon, Yale University[*]

Learning Like a State: Statecraft in the Digital Age

Abstract

What does it mean to sense, see, and act like a state in the digital age? We examine the changing phenomenology, governance, and capacity of the state in the era of big data and machine learning. Our argument is threefold. First, what we call the dataist state may be less accountable than its predecessor, despite its promise of enhanced transparency and accessibility. Second, a rapid expansion of the data collection mandate is fueling a transformation in political rationality, in which data affordances increasingly drive policy strategies. Third, the turn to dataist statecraft facilitates a corporate reconstruction of the state. On the one hand, digital firms attempt to access and capitalize on data "minted" by the state. On the other hand, firms compete with the state in an effort to reinvent traditional public functions. Finally, we explore what it would mean for this dataist state to "see like a citizen" instead.

Keywords: state, government, digital economy, machine learning, automation, algorithms

I. Introduction: The New World of Statecraft

Modern bureaucracies, whether public or private, derive their power from information. In James Scott's (1999) influential formulation, the high modernist state imposes rationalization to force populations and the environment to fit its abstract, orderly designs. In this view, states are constellations of office and field workers, executants and planners, front desk bureaucrats and specially trained experts, who join together in one long chain of actions to perform the considerable work of classification, identification, and measurement that makes the world legible, prepares it for intervention, and sustains the functions of government. What states know, then, depends on the design, reliability, and coherence of this vast socio-technical machinery as it interacts with its targets. However it turns out in practice, the process by which states come to see is a special kind of power that has been variously criticized as intrusive, imperfect, unjust, and oppressive. Further, the state's centralizing nature raises the specter that an organization managing such large troves of information, no matter how dispersed across agencies, inherently harbors a propensity for totalitarian control (Harcourt 2015).

Capitalism, too, thrives on an "immense accumulation of knowledge." From the scientific management of the labor process to the record-keeping activities of commercial organizations to the mundane collection of every bit of digital data, surveillance has a long history in the market as well (Bouk 2015; Aronova et al. 2017; Lauer 2017). Firms routinely use information to make their

[*] For correspondence, please email Marion Fourcade (fourcade@berkeley.edu) or Jeffrey Gordon (jeff.gordon@yale.edu). We thank Fleur Johns, Angela Harris, Aziz Huq, Margaret Somers, and two anonymous reviewers for their excellent comments. David Joseph-Goteiner and Carolyn Yang provided excellent research assistance.

production process more efficient, to extract value from knowledge, to identify and precisely target opportunities for profit, and to sort people and things according to value expectations (Gandy 1993; Fourcade and Healy 2017a). Information, increasingly, has become a corporate asset, to be valued on its own terms for the stream of services that it generates (Birch 2019). Modern digital corporations boast about the millions of people in their databases, about the thousands of data points in each individual profile, or about the range of topics covered by these data points. For instance, the data broker LiveRamp (formerly Axciom) trumpets that its flagship product, InfoBase, "is the largest collection of U.S. consumer information available in one source with over 1,500 attributes representing 100% of marketable US consumers and households." Shoshana Zuboff (2019) recently coined the term "instrumentarian power" (an analogy to totalitarian power) to capture those totalizing ambitions that are deployed in the market and for commercial gain—rather than in the state and for biopolitical control.

Notwithstanding these conceptual distinctions, the biopowers of the state and the market have always been hard to disentangle in practice.[1] Because distribution and coercion are central to economic life, political judgments legally constitute and shape the economy, even as conventional discourse insists on a public-private divide (Britton-Purdy et al. 2020). And while citizens generally recognize a practical boundary between services offered and authority imposed by private firms and the state, respectively, that boundary is often blurred, as in the "divided welfare state" where public and private social benefits exist side by side (Hacker 2002), or in technological development, where innovations from the iPhone to biotech ride on government investments (Mazzucato 2013; O'Mara 2019). Whether forms of public-private overlap extend or weaken the state's capacity and authority is an empirical question, however. Someone living in the United States, for instance, may feel that anything about them is for sale: "[T]he line between governance, surveillance and private life is evaporating. What we face today is one unified marketplace. . . . . Governing is collapsing into commerce . . . . And commerce is turning into governance" (Harcourt 2015, 188). The same person living in China, on the other hand, may have a reversed perception, and develop a heightened awareness of the heavy demands that the government places on private companies in an effort to bolster a unified population-surveillance project (Cheung and Chen 2018).

Public and private commingle at the frontier of technological change. They commingle when companies "move fast and break things," subverting the rules of the economic, social, or political game and the regulatory power of the state (Zuboff 2019). They commingle when private empires emerge from a relationship of dependency with the state's financial power (O'Mara 2019), or piggy-back on its record-keeping functions in the domains of property and tax, family relations, licensing, ecological or climate monitoring, and more. They commingle when corporations peddle their business to public agencies, sifting aggressively through their data to promise better and more efficient management—and possibly making armies of state agents irrelevant in the process. Finally, public and private commingle when private firms or "philanthropo-capitalist" ventures offer alternative visions of governance in traditional public-good domains like education, transportation, or health, over which they aspire to exert sovereign, state-like power (Giridharadas 2018): power that claims universality (reaches everyone), comprehensiveness (reaches deep), indefinite temporality (never expires), and circularity (i.e., whose exercise feeds back toward its original source). Many of these companies are global, defining new territories of influence that challenge national supervision.

The broader context of these transformations is important. They arise from the new possibilities afforded by technology, as well as from a four-decade-long (and very much ongoing at the time of this writing) reorientation of the state to serve the market, by means of fiscal shrinkage, re-regulation,

[1] Biopower is a form of power "bent on generating forces, making them grow, and ordering them, rather than one dedicated to impeding them, making them submit, or destroying them" (Foucault 1998, 139).

privatization, and symbolic degradation (Farrell 2018; Prasad 2018; Lewis 2018). Government institutions (including municipalities, school districts, counties) often find that they lack the material resources and the technical expertise to either take advantage of their existing data troves (whether analog or digital), or to generate new, data-rich control tools. As a result, they often delegate the manufacturing of these devices and functions to external organizations. For instance, criminal courts throughout the United States are grappling with a risk-assessment instrument developed by a for-profit company, Northpointe Inc. (Christin 2017). In many cities, law enforcement agents rely for their daily work on a platform-based intelligence tool developed by the software company Palantir (Brayne 2020). Government agents, particularly those in low-status positions, are increasingly bound by the decisions of machines—from scores that summarize life histories to red flags that prompt investigations or deny benefits, to numerical thresholds that trigger automatic warnings (Eubanks 2017).

What may first appear as mere shifts in the state's use of technology actually heralds a deeper transformation in statecraft itself. This article investigates what happens to the state—-its structure, its operations, its politics—as the new technologies of control are being actualized. Michel Foucault (2010) and Wendy Brown (2015) have reminded us to understand neoliberalism as a set of political rationalities, not just a set of market practices or economic policies.[2] According to Brown, neoliberal governmentality is a response to the question of how to govern in a space inhabited by *homo economicus*, the economic subject. Similarly, we aim to draw attention to the unique form of rationality required to govern a new subject: what Gilles Deleuze (1992) called the "dividual," the subject as seen through slices of data from particular aspects of his life, such as health, finances, or education. While statistics was the technique of choice of neoliberal governmentality, the emergent political rationality we identify is philosophically dataist and progresses through the deployment of new computational tools. The most prominent of these is a class of computing algorithms known as "machine learning." Designed to infer the discovery of rules and patterns from data, these algorithms are widely used to automate a large number of routine tasks and organizational decisions—including in government agencies (Domingos 2015).[3]

Our argument unfolds in three moments. First, we show that as machines take over significant parts of the state's operations, the role and social position of state officials undergoes a profound transformation. What happens to them is what happens to any industry facing automation. They might shrink as a group. With their actions increasingly constrained by silicon oracles, they lose the discretion that was the basis of their social power. Their expertise is demoted and cheapened. How the state is *experienced* by citizens also changes. As technology increasingly frames matters of day-to-day governance, politics fades into the background. The state also becomes more impenetrable, less accountable, possibly triggering a crisis of legitimacy (Citron and Calo 2019).

In the second part of the paper, we turn to changes in the nature of governance. The focus of state interventions has now moved from seeing the population through broad, man-made categories to seeing it as an all-encompassing web of dividual data flows to be processed (Cheney-Lippold 2017). Through data-hungry techniques of machine learning, a new world of statecraft emerges, whereby the state (and its contractors find themselves compelled to not only seek and demand new kinds of data, but also mine it in a somewhat agnostic fashion to find the relations that stick. It is no longer necessary to flatten society to make it legible (as high modernism required); instead, ubiquitous data capture (both acknowledged and secretive) means that identification and legibility can be produced algorithmically—that is, categories emerge organically from regularities observed in the data (Cheney-

[2] As Jamie Peck (2010) observes, there have always been a set of divergent, yet, related, national forms of neoliberalism.

[3] This paper focuses specifically on machine learning algorithms, but also discusses the broader automation of government tasks, some of which relies on more traditional forms of computing and statistical inference.

Lippold 2017). New ways of "sensing" and knowing (Johns 2017), new metrics for measuring fitness or difference, and new governance forms based on cybernetic feedback loops—which not only work on their own but *design their own social purposes*—come into view as the abundance of data expands some possibilities, while staff scarcity shrinks others (Amoore 2013).

We term this new form of governmentality the dataist state.[4] We borrow the concept of dataism from Yuval Noah Harari (2017, 428), who writes that "[d]ataism declares that the universe consists of data flows, and the value of any phenomenon or entity is determined by its contribution to data processing." Harari proposes dataism as an ascendant belief system, a possible successor to humanism. From our perspective, dataism is just as much a philosophy of governing. This philosophy declares that a society consists of data flows, the state's responsibility is to collect and process that data, and a well-governed society is one in which events are aligned to the state's models and predictions, no matter how disorderly in high-modernist terms.

For all the soaring ambition of this vision, the methods and rationale of the dataist state are not uniquely its own. In the next two sections, we observe that the dataist state may be vulnerable to competitive challenges from any institution that can claim to make better predictions or deliver better outcomes. To be sure, corporations have long been involved in the delivery of state services (Schick 1970). But in the new world of statecraft they do more, having designed the very categories (the bits of information) through which both states and markets now apprehend the world (Cheney-Lippold 2017; Fourcade and Healy 2017b). The state may be uniquely capable of "minting" data—we suggest several parallels between the production of data about citizens and the production of currency—but that data tends to leak out into corporate hands, where it is redeployed for profit-seeking ends. As a result, corporations routinely face the state-like work of organizing and maintaining the basic social contract that links citizens to one another, and to a putative higher authority—which may be, in the end, none other than corporations themselves.

Dataism is not an inevitable consequence of using data in governance. It is an ideology that finds the purpose of government in what can be measured rather than in the will of the people. In our conclusion, we suggest an alternative vision for the state in the digital age: a mode of statecraft that we call *seeing like a citizen*. Seeing like a citizen means identifying social problems from the perspective of those affected. The tools of big data analysis may be powerful aids for that project, but only if paired with legal and political arrangements that empower those governed to decide what should be measured, how, and to what ends. We draw attention to several recent proposals—grouped under the banner of "digital socialism"—for doing so.

II. Automation and the Changing Phenomenology of the State

We have come a long way from the time when social theorists hailed the impartiality of the well-trained, rule-bound government agent as a guarantee of procedural fairness. The ideal-typical bureaucrat, Max Weber (1946) wrote, was rational, objective, acting only by the rule and "without regard for persons." Fairness was embodied in the person of the civil servant, trained to exert his judgment in a highly codified and disinterested manner. He was likely to be male, to enjoy a stable and elevated social status, and was rather well paid. But he was not perfect, far from it: sometimes corrupt, often prejudiced, frequently incompetent, and looking out for his own survival above everything else. So, it would seem that his replacement by a computer should deliver us from his failings—that the cold, mechanical objectivity of mathematics should be a cause for celebration.

[4] Our view here is close to Cuéllar and Huq, who have recently used the term "machine learning state": "a nation state with sufficient bureaucratic and technological capacity to rely extensively on machine learning techniques for surveillance, enforcement, and security" (2019, 2).

And yet to a scrupulous observer, this shift of authority from "disciplinary" to "mechanical" objectivity (Porter 1996), from "persons to machines" (Pasquale 2018)—or, more often, human-machine assemblages—is delivering something else that Max Weber also foresaw: "an unreal realm of artificial abstractions, which with their bony hands seek to grasp the blood-and-the-sap of true life without ever catching up with it" (Weber 1946, 141). As the locus of administrative decision-making shifts toward software, the complexities of "true life" must fit analytical categories imposed by the state, whether blunt or precise, in order to be made relevant. And as the number and complexity of these classifiers grows, human discretion may be seen as increasingly inaccurate or illegitimate. In her rendition of the rise of automation in social services for the poor, Virginia Eubanks (2017) observes that the frontline agent (who is now more likely to be female) is disappearing. She now second-guesses herself when the computer renders a verdict different from her own analysis of a case. Bit by bit, she is being turned into an executant, her work de-professionalized and Taylorized into discrete tasks. Decision by decision, she is forced to detach herself emotionally from the people she is supposed to serve. She fears becoming irrelevant and worries about being downsized—although in practice some frontline bureaucrats find ways to "sabotage" or work around the systems in which they are meant to cooperate (Raso 2017; Kellogg et al. 2020).

The highly rationalized state featured a strange mix of rule-bound and embodied judgment. Under a "rule of persons," decisions are made socially authoritative and trustworthy in two primary ways: *ex ante*, through the guarantees offered by professional training, standards, and ethics; and *ex post*, through the possibility of retrospectively interrogating agents' reasoning. Phenomenologically, though, it is not rules but tacit knowledge that is the mark of the expert's skill. The most experienced and accomplished professionals are those who have the ability to make immediate, un-reflexive, situated responses. As Dreyfus and Dreyfus put it, "[N]o amount of rules and facts can capture the knowledge an expert has when he or she has stored experience of the actual outcomes of tens of thousands of situations" (2005, 788).

It is precisely this tacit dimension of skill that Dreyfus and Dreyfus thought (as late as 2005) fundamentally separated machines from humans.[5] Because machines needed operating rules to arrive at outcomes, they could never become fully "expert." This seemed to place a limit on the decades-long effort to construct artificial intelligence in the form of "expert systems" (Brock 2018). But that was then. Today's artificial intelligence is able to replicate not only the rule-like procedures that structure professional decisions, but also, in some domains, the tacit skills through which both experts and laymen come to *see and decide*. The practical successes of a new paradigm for teaching computers in domains as varied as game-playing (chess, Go, video), image and language recognition, or (in some contexts) risk prediction make it difficult to distinguish human intelligence on the basis of tacit knowledge alone. This new paradigm is machine learning. Modern machines, whether trained on large amounts of curated and labeled data or unstructured data, decide the rules of classification and decision-making on their own, much like human brains. In many areas, machine-learning algorithms now perform not only better than rule-based ones, but also better than human experts. This is true for narrow prediction and classification tasks (e.g., in finance or medical imaging), and increasingly for constructive tasks as well (e.g., writing software).[6]

The phenomenological implications of what Mariano-Florentino Cuéllar (2017) calls "cyberdelegation" (the delegation of administrative agency decisions to artificially intelligent systems)

[5] "In each area where there are experts with years of experience, the computer can do better than the beginner, and can even exhibit useful competence, but it cannot rival the very experts whose facts and supposed heuristics it is processing with incredible speed and unerring accuracy" (Dreyfus and Dreyfus 2005, 781-782).

[6] The benefits are sometimes marginal, however, particularly when the goal is to predict human behavior (Narayanan 2019).

are not trivial.[7] The state's growing internet presence, and its dispersed and outsourced human infrastructure, have resulted in it feeling simultaneously more intimate and more remote. In some ways, the state is now right there at one's fingertips. Anyone with a working internet connection can interact with it through a computer or mobile interface. The proliferation of public-facing government websites and platforms also creates a feeling that the state's actions should be more easily knowable, if only by establishing an aesthetics of transparency (Valverde, Johns, and Raso 2018). So-called "open data" initiatives, whereby state agencies make a profusion of information available online in machine-readable format, are often implemented in the name of transparency and accountability (for example, see Björklund [2016] on e-government in Estonia). But such outcomes are by no means a certainty: if the information that is so broadly shared is essentially mundane (e.g., bus schedules) and not politically sensitive, the "technology of open data" is unlikely to translate into a "politics of open government" (Yu and Robinson 2012).

Furthermore, even transparency has a downside: it intensifies vulnerability to heteronomous pressures (economic or political). Increased scrutiny of judges via judicial analytics, for instance, might exacerbate legal inequalities by providing those with money yet one more way to select the most favorable forums, eroding trust in the impartiality of the justice system and, consequently, accelerating reliance on automated tools as a defense against the very suspicion that this is occurring. Finally, treating the state as a platform for various private services may open the door to private appropriation of public data and, consequently, the generation of private claims on public functions (Lewis 2018). Cost-cutting strategies within the state (particularly aggressive under the presidency of Donald Trump) may accelerate the shift. For instance, the Internal Revenue Service recently signed a contract with Palantir to pursue tax cheats using data mining technologies. A Bloomberg report notes that the contract "comes at the end of a period when the Internal Revenue Service lost hundreds of special agents to budget cuts while being overwhelmed by data volume that reached the equivalent of 1.5 trillion text files last year, a tenfold increase in a decade" (Bulusu 2018, n.p.). This sort of partnership raises concerns both as to what the private partner will do with this data, and whether the laws of government transparency will apply to it.

Even when it seeks to be "open" or "transparent," the state is also becoming physically distant. Its infrastructural footprint has already been declining for decades.[8] And much of the digital state, just like the large digital corporation, resides in massive servers tucked away in rural areas. What the Snowden dossier exposed, for instance, is that today's National Security Agency is, at least metaphorically, a gigantic network of tubes that leads to the Bumblehive, a massive data processing center in the middle of Utah. Just like the large digital corporation, the digital state may someday employ a fraction of its current workforce and rely on data janitors (Gray and Suri 2019) to clean the innumerable inputs that feed automatically into its cloud.

While digitality broadens the scope of state action, increases its efficiency, makes services more accessible to a wider range of people (particularly those with few resources), and possibly (if properly calibrated) reduces bias (Kroll et al. 2017), its workings are opaque, certainly to laymen but also, increasingly, to experts themselves. The gap between the practical advances enabled by machine learning techniques and their lack of accessibility to human reasoning (Burrell 2016)[9] creates a real

[7] Also see Coglianese and Lehr (2017).

[8] In 2016, the share of civilian federal government employment as a percentage of the total workforce was at its lowest since 1959 (Shapiro 2017). The number of US Postal Service offices peaked in 1901 and has declined continuously since then. See US Postal Service, Pieces of Mail Handled, Number of Post Offices, Income, and Expenses Since 1789, https://about.usps.com/who-we-are/postal-history/pieces-of-mail-since-1789.htm.

[9] This is due to humans' inability to conduct mathematical optimization in high-dimensional space.

political conundrum: the artificially intelligent state—just like the artificially intelligent corporation—increasingly lacks the technical ability to account for its own actions, including to itself.[10]

This state of affairs may play out in several different ways for those who are on the receiving end of administrative decisions. The "de facto delegation of rulemaking power" (Citron 2008) to machines imparts their decisions with a mystical aura and apparent intractability that is often hard to question. This is in spite of the fact that the quality of algorithmic risk predictions is eminently questionable, and that their methods are known to be insensitive to essential institutional norms (such as due process in the legal system) (Liu, Lin, and Chen 2019). Not only do databases frequently contain mistakes ("garbage in, garbage out"),[11] but data collection is often tainted by institutional stigmatization and discriminatory treatment (O'Neil 2016; Noble 2018; Benjamin 2019). The problem is made worse by the aforementioned difficulty of interpreting outcomes. This "black box" characteristic of machine learning tends to further fuel magical thinking and institutional obfuscation.

Building on a long tradition of using numbers to shield their actions from public scrutiny (Porter 1996), state actors may now find themselves in a stronger position to claim their subordination to computers and their inability to account for their decisions (since both claims will presumably be true). This peculiar power of unintelligibility to erode responsibility and deflect criticism may extend even to cases where artificial intelligence is not at stake. When a new budget tool slashed the Medicaid benefits of a group of disabled people in Idaho, it took "four years, four thousand plaintiffs, and a class action lawsuit [by the ACLU] to get to the bottom of what had happened:" the culprit, it turns out, was a series of gross mistakes on a simple spreadsheet (Fry 2018, 17). The "algorithm" was not the source of the problem, but as a myth of how the state works it offered political cover and undermined the need to give an account.

Of course, the administrative state has long been subject to criticism for being cloistered, opaque, or unaccountable to the public. The project of administrative law has been, in large part, to meet these charges. Thus, notice-and-comment rulemaking requires federal agencies to respond to all cogent arguments made by members of the public and to explain why they have chosen a given rule over plausible alternatives; judicial review of agency adjudication gives affected parties a chance to challenge agency decisions; and transparency procedures like the Freedom of Information Act help to unearth internal agency proceedings.

As the administrative state becomes more algorithmic, these procedures will require new analogues specifically suited to statistical decision-making. Scholars commissioned by the Administrative Conference of the United States have argued that algorithmic decision-making, by encoding legal principles and bureaucratic priorities, might create a more substantial public record for affected parties to challenge in notice-and-comment rulemaking and in court than does the status quo (Engstrom et al. 2020). But the authors also note that the existing principles of administrative law, which treat a rule or a decision as fixed over time, may be inadequate for reviewing algorithms that change as they are trained on new data. They therefore recommend retrofitting the Administrative Procedure Act, to create new principles for reviewing algorithmic decisions; to create AI oversight boards within agencies; and to require agencies to engage in "benchmarking" by comparing AI-assisted and human decisions. In a similar vein, Huq (2020, 619) proposes that regulated parties should be entitled to "a right to a well-calibrated machine decision" that incorporates due process, privacy, and equality values.

[10] Furthermore, the state's opacity might grow precisely as that of citizens decreases: the more data people relinquish, the more the state may be able to use technologies—like neural networks—that render its decision-making process less transparent.

[11] Once inaccurate information starts circulating and duplicating itself throughout the digital ether, correcting it may be difficult and time-consuming, demanding technical skills and financial resources that few people possess or are willing to commit (Eubanks 2017).

We view these proposals as a good start. But we caution that there is a difference between holding the state to account for its decisions—i.e., as justified on the basis of the available data—and holding the state accountable for what sort of data it collects in the first place, and what worldview or governmentality follows from doing so rapaciously and indiscriminately.

III. Dataism and the Changing Nature of Control

Most organizations today will regard the collection of data as a natural part of their social essence, a well-institutionalized cultural imperative to which they submit themselves ritualistically (Fourcade and Healy 2017a, 16). Once armed with the proper technical know-how, any institution will seek to generate, scoop out, store, and "assetize" (Birch and Muniesa 2020) as much information as possible, sometimes without specific end uses in sight. Repeated scandals in both public agencies (e.g., the PRISM program at the NSA) and private companies (e.g., Apple's contractors listening to their users' conversations) also suggest that these strategies prevail whether or not they are authorized. Besides, indiscriminate surveillance is easier to implement than carefully targeted surveillance. Once in place, however, the abundance of data defines new strategies of action guided by the purposeful, yet increasingly agnostic exploration of data and metadata.

The rise of the modern state exemplifies this tendency. Statistics—the science of collecting, organizing and interpreting data—was first and foremost a science made by and for the state (as the German cameralists knew all too well). Since at least the seventeenth century, much of the state's world-making power has been dependent on its growing monopoly over the classification, measurement, and record-keeping of information in multiple domains of economic and social life, and on the truth effects projected by these activities (Bourdieu 2015). But *how* the state abstracts, makes sense of, and acts in the world is the outcome of contested socio-technical processes that are situated in time and space (Desrosières 2002). The displacement of analog technologies by digital ones, as well as emergent forms of computation, are defining new affordances and possibilities for state bureaucracies to see, sense, and act.

We can discern what is distinctive about the dataist state by comparing it to older forms of statecraft, like the high-modernist state studied by James Scott and others. Grand in ambition but poor (by today's standards) in information-processing capacity, the high-modernist state forced its subjects into blunt, overbroad categories; its distinctive failures came from overgeneralizing and denying local differences. In the realm of civic planning, for example, cities like Chandigarh and Brasilia embodied the high-modernist approach to urban life (Scott 1999). Regularized street grids made navigation easy. Activity-based zoning anticipated the categories of human experience and allotted separate space for each: residence, commerce, leisure. Streets were built to the width of maximum expected traffic volume, ensuring that there would never be congestion. These planning decisions were the hallmark of a state determined to provide the means of flourishing for its population, but insistent that none of that flourishing take place beyond its gaze. Dark, dense alleys and unnumbered shops and homes were unacceptable because they were "illegible," or too difficult to monitor or even count. Planning was therefore the state's prime opportunity to guarantee a city fit for measurement: the dimensions would be fixed in concrete.

The idealized city of the dataist state reverses this sequence of events. Rather than planning a city sized for a certain population, certain traffic, and certain activities, planning follows *after* urban life commences. Public amenities must be fluid and responsive. But it would be a mistake to view fluidity as incompatible with predictability or legibility. Scott was correct to identify a state's fundamental need to make legible any territory that stretches beyond the personal familiarity of its agents. But machine learning algorithms aspire to make even the fluid legible—that is, essentially, to classify it. In its now-defunct vision for Toronto's Waterfront district, Google-affiliated Sidewalk Labs proposed to use "ubiquitous sensors [to] feed data into automated street design, turning streets as needed into conduits for bikes or pedestrians or priority vehicles" while "[r]esponsive applications built on top of the platform [were to] deliver services (from food to sanitation to work space) 'just-in-time' for public consumption" (Goodman and Powles 2019, 23).

Scott's critique of high-modernist planning would have been inapplicable to Sidewalk Toronto and many other contemporary development projects utilizing iterative, provisional mock-ups—what Fleur Johns (2019) calls "prototypes"—rather than rigid plans. This project and others like it boast responsiveness as their leading quality. By discovering what—and who—they can reliably predict, data analysts inductively raise possible interventions the state might make into the world, not only to achieve existing goals, but also to define new goals through "smart" instruments. And even when the dataist state pursues pre-existing goals articulated by humans (e.g., public health), it differs from the high-modernist state by operationalizing those goals in emergent, speculative constructs of the data (e.g., personal fitness tracking activity or Google searches for certain symptoms). What the high-modernist and dataist states nonetheless share is a top-down, hierarchical relationship between the technocrats who plan or nudge society and the citizens who inhabit it.

What kind of state, then, emerges from conceiving of the citizenry, material infrastructure, and nature itself as so many streams of data? And what are the distinctive advantages and blind spots of this way of seeing? We make three points. First, the dataist state models its population as a set of fluctuating, always emergent patterns. It perceives social problems in terms of individual rather than collective causes, and manages through behavioral manipulation. Second, the temporality of the dataist state is oriented to the near future: that is, the future that can be predicted on the basis of available data. And third, the dataist state's measurements and rankings enable it to distinguish differences between people. In the hands of the state, such distinctions principally facilitate means-testing. But they may also facilitate the deployment of authoritarian forms of political control, or serve as a Trojan horse by which corporate interests subvert the state's data troves for the sake of price discrimination and value extraction.

A. The Dataist State Is Behaviorist

The dataist state develops its picture of the world by collecting data from both inanimate things (man-made and non-man-made) and from living beings (people, plants, animals, viruses, bacteria). As stated above, much of the logic behind this impulse is possibilist ("because we can"). But there is more to it than that. The dataist state, unlike the neoliberal state, does not seek to produce a rational economic subject—a *homo economicus*. Its purpose, rather, is to obtain the desired behavior, whether or not it is animated by rational intentions. If "behavioral biases" and "irrational" emotions are the way to obtain this alignment, then they are fair game (Fourcade 2017). Sunstein's "nudge" framework, for instance, understands governing to be about *dispositifs* that guide individuals to make desirable choices regarding their health, behavior, and personal finances. Critics may disagree whether such paternalism is really benevolent (Sunstein 2015), but here we simply emphasize that it frames governance as a design problem and that it takes dividuality—slices of individual behavior—as the most pertinent unit of analysis.

Social problems that involve group decision-making are less suited to this behaviorist approach, let alone distributional problems where the cause may not be "irrational" or undesirable behavior so much as entrenched, structural disadvantage. Giorgio Agamben diagnoses a shift in states' ambitions to confront difficult problems "whereby the traditional hierarchical relation between causes and effects is inverted, so that, instead of governing the causes—a difficult and expensive undertaking—governments simply try to govern the effects" (2014, n.p.). Governing the effects often means striving to identify which people are vulnerable to a social problem—illness, gang membership, medical bankruptcy—and triaging resources their way, even at the expense of attacking the underlying problem. It also requires subjecting the entire population to invasive surveillance, since everyone is a potential candidate for such interventions. In this way, Evgeny Morozov observes that intelligence services have "reduced the topic of terrorism from a subject that had some connection to history and foreign policy to an informational problem of identifying emerging terrorist threats via constant surveillance" (2014a, n.p.).

If the first limitation on behaviorist statecraft is that individual behaviors reflect only a small subset of deserving social problems, the second limitation is that an inductive, reactive state can deal only with the even smaller subset of individuals captured by its measurements. By inductive, we mean that the state sets its goals at a high level of abstraction, and lets exploratory data analysis bring the more proximate goals into view (Dewey 1939). For example, city health inspectors have partnered with Google in a pilot program that would make restaurant inspections follow inductively from residents' Google searches about symptoms suggesting food-borne illness (Sadilek et al. 2018). Contrast this approach with one that starts with the restaurants and proactively mandates food safety procedures. The two approaches are not mutually exclusive, but they do represent opposite theories about when the state should intervene: before problems arise, or afterwards.

Inductive statecraft is especially vulnerable to imperfect data. In the case of detecting tax evasion, for example, Italian bureaucrats have experimented with "the redditometro, or income meter, a tool for comparing people's spending patterns—recorded thanks to an arcane Italian law—with their declared income, so that authorities know when you spend more than you earn" (Morozov 2014a, n.p.). But while such data may be useful for identifying tax fraud on the scale of under-the-table, all-cash businesses, it would be useless against billionaires who evade taxes through offshore trusts and whose consumption is unlikely to exceed declared income under any circumstances. Morozov concludes that "[a]lgorithmic regulation is perfect for enforcing the austerity agenda while leaving those responsible for the fiscal crisis off the hook." More generally, the dataist state punishes and rewards its citizens on the basis of what parts of their lives show up in its databases. The quest to garner (or avoid) state aid becomes as much about being seen—or staying invisible by avoiding government institutions (Brayne 2014)—as about the substance of one's actions.

B. The Dataist State Is Experimental and Opportunistic

We have argued that the dataist state's "line of sight" (Amoore 2009) is framed by its dividualist and behaviorist approach to social life. Here, we further argue that this emergent governmentality eschews fixed, long-term plans in favor of a constant state of real-time experimentation and reactivity to indicators, as if working through a dashboard.

This experimental attitude is, in part, a response to the complex, unpredictable, emergent risks that modern states strive to manage. Julie Cohen (2016, 17) observes that the industrial-era regulatory landscape—where harms were "clear and concrete"—has been replaced by the regulation of "systemic threats" (including disease, financial collapse, and ecological devastation) that are accessible only through probabilistic modeling and representation. In the face of threats that unfold either gradually over many years (e.g., climate crisis) or rarely but catastrophically (e.g., financial crisis), the state now aims its regulation at intermediate targets or "leading indicators" (Aradau and Van Munster 2007; Lakoff 2007). These indicators cannot answer the question of whether the longer-term threat has been averted; indeed, threats like terrorism, climate crisis, and financial panic are not so much to be averted as anticipated and managed. But the lack of satisfying answers may lead the dataist state to settle for metrics that at least yield the satisfaction of predictability.

Importantly, the new perceptions of threat or risk are not independent from the new data regime. What can be measured is managed. But what can be measured is not necessarily what really matters. The institutional relevance of measures is often defined by affordability, ease of collection, or political preference rather than by real-world pertinence. The long-lasting structural inequities embodied in historical datasets, such as those commonly used in police and judicial algorithms, potentially reproduce stigmatization and injustice (Benjamin 2019). For instance, the poor are much more likely to be surveilled than the wealthy, and white supremacists may be less likely to end up on a "terrorist" list. Finally, more often than not, usable measures propose an inaccurate representation of the underlying policy goal.[12]

Second, what can be measured changes and grows as new data sources and new computational techniques come along, and so the state finds itself pursuing a moving target of social control and regulation. In a database of potential "terrorists," for example, it may be that the same individuals are flagged as threats over a period of years. This opens a horizon on which the state can plan. But if the predictions are fleeting-–and deemed urgent-–the state may feel compelled to act immediately. In this way, the short interval between analysis and action leaves the state in a constant state of preparedness: ready to react to a continual stream of new threats and opportunities emerging over the horizon (Amoore 2009).

In a study of a digitally attuned NGO, Fleur Johns draws out the differences between those (high-modernist) agencies that impose well-defined plans and those that prepare for unknown futures:

> By and large, Pulse Lab Jakarta fosters an open-ended, opportunistic, now-oriented disposition of a kind that has been identified with entrepreneurship. To the extent that this present orientation entails leaning towards a future, it is "a near future, a future with limits", with those limits defined by the "temporality of the project"—that is, the project to develop or trial a particular, prototypical application or assemblage of digital data for development purposes (Johns 2019, 850-51).

Johns stresses that the limits on imagining such futures come from the data: this form of reason "envisions possibilities being worked up iteratively and inductively from the inferences that may be drawn from the data available, as limited or partial as those data may be, rather than through cross-sectoral information-sharing, experimentation and learning" (853). Even when data are complete (in the sense of covering the whole population), moreover, they may only be valid for predicting events in the near future.

C. Biopolitics of the Dataist State

Fundamentally, states deploy digital tools in order to identify, surveil, and manipulate individual bodies in real time. Far from decentralizing control, the digitization and algorithmicization of identities (electronic, biometric, and now genetic) offers the ability to link all pertinent information in a central register or to create protocols that enable information-sharing between administrative units, including across national borders. Governments have been eager to develop such systems in an effort to modernize or expand the delivery of their services, with many poorer countries (such as India) resolutely leapfrogging analog technologies. This transition outlines a new kind of biopolitics oriented

[12] In the United States, for example, frequently used proxies that were claimed to predict health needs, crime, or child harm were found to measure health costs (Obermeyer et al. 2019), police activity (Robinson 2018), and bureaucratic decisions (Eubanks 2017) instead. In all three cases, risk evaluations based on poor, narrow and backward-looking data reproduced past discrimination (Harcourt 2008).

to the government of populations and the production of new subject categories, with both mundane and potentially chilling "power over life."[13]

For all its behaviorism and experimentalism, the dataist state is not a weak state. Nor is it necessarily a lean one, whether in the sense of the "lean startup" ideal, which likewise works through iterative, provisional mockups (Ries 2011), or in the sense of unambitious, chastened by austerity. In fact, in both democratic and authoritarian countries, the dataist state may measure up as an achievement of political vision on par with, or exceeding, the most sweeping high-modernist plans.

Consider several examples from around the globe. The Indian government's deployment of a universal biometric identity system linked to welfare benefits, Aadhaar, turns into a civil liberties nightmare in the wake of expanding mandates, growing compulsion and cooptation by private interests (Khera 2019; Rao 2019). The U.S. National Security Agency effectively redefines American citizenship as an algorithmic achievement, based on the national- or foreign-centeredness of one's online behavior. This data-driven reconstruction, in turn, has been used to legitimate an entirely new regime of surveillance for people with a U.S. passport but suspicious foreign connections—a sort of *jus algorithmi*, as Cheney-Lippold (2017) calls it. In Singapore, the hyper-connected, datafied urban space claims to deliver orderly economic growth and social progress by producing "smart citizens"—while maintaining the power of the authoritarian regime (Ho 2016). The Chinese state announces its plan to rely on financial inclusion and the nascent infrastructure of "social credit" to regulate individual and corporate conduct, and engineer what it calls a "trustworthy society" (Loubère 2017). Under the Chinese social credit system, the public and private treatment of each person is to be directly tied to measures of good citizenship (e.g., complying with laws, paying court judgments, and honoring contracts) (Matsakis 2019). The overall undertaking is no doubt an achievement of political vision (if a deeply troubling one): full citizenship is increasingly something to be earned—and lost—through one's actions, and something that is at stake on a daily basis.

The distinctive features of China's social credit project are its totalizing scope and its forthright articulation of what ideals citizens should live up to. Different arms of the Chinese state, as well as some city governments, have stepped into the business of credit scoring, alongside commercial companies (Liu, Lin, and Chen 2019). These social credit systems are anything but "agnostic" in the sense used above. Citizens and corporations are measured with an eye toward rewarding a well-defined social ideal of trustworthiness verging on compliance, often in the service of broader social goals (e.g., to foster environmental cleanliness or punish corruption). Chinese government entities have also asked social media companies to incorporate government-created blacklists into their platforms, where individuals' blacklisted status may be shared with their contacts or used to disallow certain actions—from in-app purchases to access to government contracts (Matsakis 2019; Ahmed 2019).

Social credit systems promise to strengthen the state's ability to monitor and govern, and as such they do seem to enjoy popular support wherever implemented. The perspective of an authoritarian government equipped with robust surveillance technology, however, raises the possibility of a drift toward totalitarianism: total control over the social body and its constituent parts. The convergence of digital surveillance and the police state in some parts of China certainly raises such a possibility. China's digital systems are trained not only to monitor forbidden behavior, but also to identify, categorize, isolate, and manage entire populations deemed politically dangerous. Targeted groups include rights activists, members of banned religious groups, and more dramatically, the Uighurs and other ethnic minorities. In May 2019, the *New York Times* reported that "China is in effect hard-wiring [the province of] Xinjiang for segregated surveillance," collecting "blood, fingerprints, voice

[13] Throughout history, technologies for identifying and counting populations have been used both to sustain democracy and to destroy it, to protect some groups and to annihilate others (for example, see Black 2001 on the critical role of IBM's census technology in identifying Jews during the Third Reich).

recordings, head portraits from multiple angles, and scans of irises" from minority groups while "generally ignoring the majority Han Chinese, who make up 36 percent of Xinjiang's population" (Buckley and Mozur 2019, n.p.). The bias introduced in the data collection process by singling out the Muslim population is all the more likely to entrench discriminatory outcomes because it is systematic and deliberate. Furthermore, in the absence of democratic scrutiny and the opportunity for correction, machine learning may allow this biased classificatory logic and its consequent rule-based actions to automate and scale, to much more dangerous effect (Farrell 2019). Finally, the problem may be compounded by the fact that many of the systems trained and perfected in Xinjiang are spreading elsewhere fast. China's sprawling cities have been blanketed with surveillance cameras, and China now exports its surveillance technology throughout the world (Mozur et al. 2019; Qiang 2019).[14]

Still, authoritarian dataism is neither monolithic nor inevitable. The power of the dataist state—relative to citizens, relative to business firms—depends on the scope of the state's data access, the legal force of its classifications, and the extent to which non-state actors can check it. Of course, these legal and institutional features vary across polities. In the next section, we explore what makes the data regimes of some states more powerful than others.

IV. Data Minting and the New Face of State Capacity

The capacity of the dataist state is measured in data as well as money. States seek the ability to access more and more private data as they strive to develop more ambitious forms of population management. The more data the state acquires, the more accurately it can predict social problems and deliver useful services (or so the story goes). There is a tempting parallel between this drive to acquire data and the state's traditional extractive mandate to collect money in the form of taxes. The comparison may be apt, but only if we move past the illusion that data or money exist idly in private hands before the state comes along to collect them. Recent critical perspectives in monetary theory have advanced the view that, for governments that issue a sovereign currency, the state must lend or spend that currency into the economy before citizens can pay it back in the form of taxes (Wray 2014). On this view, taxes are necessary not because the state "needs" the revenue to pay for services, but because they sustain a demand for the currency (one needs it in order to meet the tax), because they check inflation, and because they serve various redistributionist aims.

The state cannot unilaterally print data in the same manner it prints money. But the state is in a unique position to induce the production of all sorts of data that would not be recorded in its absence. Through compulsory interactions—from policing to border security to tax collection to census taking—the state mints data. And even beyond compulsion, the state has begun to cast voluntary data sharing as a form of good citizenship. Citizens are asked to record data about events they observe, like crime; volunteer information about themselves for the public good, as in the census (while technically mandatory, effective census participation requires cajoling and encouragement); and surrender information about themselves in order to assume a state-recognized digital identity. Public agencies, like all organizations, also increasingly mobilize alternative sources as they search for information about particular individuals. This can be accomplished either informally, by snooping around the

[14] This is a dark reminder that every state, dataist or not, is always, *potentially*, a concentration camp (Agamben 1998). Some scholars see an affinity between artificial intelligence and tyranny. As Harari (2018) puts it, "once we begin to count on AI to decide what to study, where to work, and whom to date or even marry, human life will cease to be a drama of decision making, and our conception of life will need to change. Democratic elections and free markets might cease to make sense."

internet,[15] or more formally, by requiring that the recipients of state benefits disclose certain kinds of information (Eubanks 2017; Wilcox 2014), or by subcontracting the task to private providers.

The duty to share data differs from the duty to pay taxes in several key ways. First, a form of data is only useful if many people produce it. This sort of network effect is a reason why state-coerced data production is potentially more efficient than private data production (although some surveillance capitalists have had no trouble generating network effects without legal compulsion). Of course, the state must also collect taxes from many people in order to sustain its capabilities. But, second, while we typically conceive of tax payments as flowing from the property of individuals, contemporary surveillance capitalism and dataist governance have successfully framed personal information as part of a "biopolitical public domain," open for appropriation by default without the need for individuals to approve transfers of their "property" (Cohen 2018).

Julie Cohen equates the origin of this domain with the 1994 invention of the internet cookie—a protocol for identifying visitors to a website. This seemingly benign piece of software threw the individualistic frame of reference of privacy law into chaos, and personal data became free for the taking: "[W]illingness to accept at least some kinds of cookies became an increasingly necessary precondition for transacting online and participating in online communities" (Cohen 2019, 54). As a matter of legal consciousness, individuals who accept something like this public domain will not seek to enforce property-like claims on "their" data. Instead, they will yield to a presumption that data is "always-already public." This view suggests something stronger than a duty to provide data. A duty implies volition; the acceptance of a biopolitical public domain implies acceptance that the state—and perhaps private data brokers as well—are *entitled* to the information therein. Finally, while taxes are often progressive, falling most heavily on the wealthy, it may be the poor who have to share the most data with the state in order to overcome the various suspicions and biases (regarding criminality, regarding benefits use) that attach to poverty and its correlates.

Besides data minting, how else might state agencies enrich their data pools? One strategy is to coax or coerce private organizations into contributing their own data. Examples of such efforts abound, from both the authoritarian and the democratic ends of the spectrum. In China, a newly established credit consortium controlled by the People's Bank, Baihang, has been seeking to force fintech companies to "share" their troves of data about private loans. The two largest firms, Alibaba and Tencent, have vigorously pushed back against these efforts so far (Yang and Liu 2019). In the United States, the relative failure of public exhortations that private corporations harness "data for good" and share more of their data to "[supplement] public statistics and [thereby inform public sector] interventions" (Alemanno 2018) has resulted in more aggressive demands. Some cities and state governments, for instance, have gone to court to force ride-share companies to make their traffic data public (Said 2019).

And, just as the state seeks to make use of corporate data troves, so too the acquisitiveness runs in the opposite direction. A final parallel between data and money creation is the inevitability of private firms piggybacking on that which was originally minted by the state. Monetary theorists note that private financiers create private money; they extend credit that is ultimately backed by state money (Mehrling 2012; Ricks 2016). In the realm of data, private production relies on the state in a different manner. For instance, many data brokers in the United States (e.g., Lexis-Nexis, specializing in legal documents) got started in the business by digitizing reams of analog records from government departments and agencies: courthouses, DMVs, public licensing boards, county tax assessors, and the like. This publicly

[15] In March 2019, for instance, the *New York Times* reported that "the Trump administration has been quietly working on a proposal to use social media like Facebook and Twitter to help identify people who claim Social Security disability benefits without actually being disabled" (Pear 2019, n.p.).

collected data was then monetized in various ways (and sometimes sold back to the state in digital form).

The American "edtech" sector offers another good illustration of the private appropriation of state-minted data. Many educational software companies make products that streamline administrative tasks for school districts, personalize courses and tutoring (e.g., Khan Academy), and assist with college counseling (e.g., Hobsons, owner of Naviance and a suite of related applications). Sometimes the software is provided for free to early adopters within a school system, in order to recruit evangelists who will encourage their administrators to purchase the paid version. Student data (grades, attendance marks, test scores, demographic information) are obtained thanks to school personnel who initially upload them into the system, after which point the software tracks students and teachers as they interact in its proprietary online environment. Insights from these data can then be deployed to lure families or schools into premium (fee-based) services, or for targeted advertising.

As these examples suggest, the prevailing relationship between the dataist state and data-driven companies ranges from commercial cooperation to a full-blown private challenge to the state provision of services, one that threatens the state's dominion and undermines its legitimacy. The data-centric and "solutionist" (Morozov 2014b) corporation now routinely competes with or lays claims on the state for the delivery of traditionally public services and the fulfilment of core governance functions. In the final section, we turn to analyzing the current balance of power between these competing sovereigns.

V. The State-Like Corporation and the New Landscape of Profit

In order to analyze the relative powers of the dataist state and its corporate counterparties and competitors, one must first recognize that *power* itself is not as monolithic as it may have once been. Back in 1992, Gilles Deleuze argued that Foucault's disciplinary society was already on the wane, and that Foucault's central concept of the panopticon was an outdated representation of the nature and functioning of power in society. The panopticon's gaze was penetrating and centralized, or at least centered; it was "rooted" in specific and enclosed locations—the prison, the school, the factory. For Deleuze, however, power is a distributed property, more pervasive and less bounded than even Foucault had conceptualized it. Another metaphor, that of the rhizome (Deleuze and Guattari 1987), captures this new incarnation of power. A botanic life form, the rhizome presents as a ubiquitous and invasive tangle of roots and shoots. As a metaphor, it evokes the multiple and non-hierarchical dimensions of the organization of culture and knowledge production.[16] Power inheres in the constituent parts and especially in the points of passage from one modality, or node, to the next. The real source of control, Deleuze (1992) argues presciently, is the *password*, which allows this movement.

Today the internet rhizome, like its vegetal counterpart, has innumerable, distributed, and connected entry and exit points: it is made of mobile devices, sensors, databases, drones, cables, servers, and more. These artifacts "connect everything together into integrated, expansive, smart systems . . . [that] spread and creep . . . You can try to shear off parts of it, but more stems will emerge elsewhere from the mass of roots" (Sadowski 2020, 44-45). For example, it is nearly impossible for a regulator to freeze a payment on the Bitcoin network because it is a distributed collection of servers, rather than any one server, that codify each transaction. Importantly, data transfers from one part of the internet to another part take place through routine, stable lines of communication between entities bound together through complex infrastructures. As Galloway puts it, "in order to initiate communication .

[16] "To these centered systems, the authors contrast acentered systems, finite networks of automata in which communication runs from any neighbor to any other, the stems or channels do not preexist, and all individuals are interchangeable, defined only by their state at a given moment—such that the local operations are coordinated and the final, global result synchronized without a central agency" (Deleuze and Guattari 1987, 17).

. . two nodes must speak the same language. Even more than passwords, *protocols* are the real loci of power. Shared protocols are what defines the landscape of the network—who is connected to whom" (2004, 11-12).

But behind the *technical protocol* (which regulates communication between computing entities) and the password (which regulates individual passage), is another kind of infrastructure: *the data sharing agreement* (DSA), a *legal protocol.* Data sharing agreements define what data are being shared and how each counterparty may utilize it. They regulate the terms of exchange, i.e., who can do what with data, and at what cost. State entities are deeply involved in these contracts as parties to DSAs with technology vendors, as enforcers of certain privacy-oriented statutes like HIPAA and FERPA, and as arbiters of contract law, reinterpreting the terms of privacy and ownership as applied to "shared" data. Tracing the sites of power in the internet rhizome requires paying close attention to how these protocols work and whom they serve. For instance, DSAs are instrumental in powering network effects, by creating chains of reciprocal obligations between individuals and private firms, between corporate entities, and between firms and public agencies (Fourcade and Kluttz 2020).

Data sharing agreements between corporations and the state must balance governance goals with privacy protection while maintaining the interests of each party. For instance, the data-fusion firm Palantir, whose customers include governments around the world, claims to be in the business of processing its clients' data, rather than generating surveillance data itself. But as private corporations enter the business of extracting information from state-collected data (often matched with data from other sources), the most interesting question may be: who can claim title to the raw materials, intermediary analyses, and final products? What happens when the state "shares" its own structured and unstructured data with private firms (as in the British National Health Service's partnership with Amazon, for instance), who in turn share it with third parties?[17] Should we think about this as a private appropriation of public data? What about users who share confidential information traditionally made for state consumption, such as their tax returns, with private corporations?[18] The crafting of data-sharing, data-pooling, and data-matching agreements between organizations may be one of the most active areas of contractual innovation today (Mill 2020).

A second development is the wholesale edging-out of the state from the business of data production. For much of its history, the modern state provided the categories that anchored corporate analysis and action—from economic statistics to social security numbers, from accounting standards to occupational nomenclatures. But this relationship is on its way to being reversed today. The AI company QuantCube, for instance, "measures economic growth in the world from 'alternative data' extracted from social media, search engine queries, GPS coordinates or satellite images" (Bouissou 2019, n.p.). Confidence indicators formerly assembled through surveys are replaced by sentiment analysis drawn from social media. The state increasingly sees through the eyes of the market as it imports privately generated tools into its governance apparatus. For instance, in a move reminiscent of developments in China, the US Department of Homeland Security stated in August 2019 that it would, under a new public charge rule, start using credit scores to determine the eligibility of immigrants applying for a green card or for US citizenship (Andriotis 2019). And the day may not be far off when the state, too, will start slotting people into categories commonly used by digital marketers.

[17] The contract allows Amazon access to information "on symptoms, causes and definitions of conditions," and "all related copyrightable content and data and other materials . . . Amazon . . . can then create 'new products, applications, cloud-based services and/or distributed software', which the National Health Service would not benefit from financially. It can also share the information with third parties." (Walker 2019).

[18] For instance, Intuit, the company behind the popular TurboTax software, has encouraged users to opt in to share their tax information with third parties in the hopes of receiving attractive loans or refinancing terms.

The consequences of these changes are not trivial: the symbolic downgrading of the nation-state as the legitimate (and monopolistic) producer of statistical truth provides a powerful argument for those who crave its material downgrading. In other words, administrative downsizing may be a natural political answer to the looming irrelevance of state functions. As Taylor and Broeders (2015, 229) observe, we are witnessing a broader "power shift from the traditional collector and user of statistics—the state—to a messier, more distributed landscape of governance where power accrues to those who hold the most data." Furthermore, digital firms' ability to collect such data on a global scale is appealing for those institutions that seek globally standardized measures (like international institutions and multinational corporations). The work of organizational isomorphism and international aggregation that the United Nations or the World Bank performed in earlier eras is on its way to being offloaded onto global private actors.

Corporations, meanwhile, frequently act as "proxy sovereigns" (Amoore 2013), or constitute "knots of statelike power" (Harcourt 2015, 215), sometimes serving as proxies of the state to enforce laws and sometimes governing conduct in ways that have law-like effect[19] (Rose and Valverde 1998). Larry Lessig (1999) argues that the architecture of cyberspace, or code, regulates conduct just as law does. Cyberspace must be viewed as a space of joint public and private governance, with its architecture built and maintained by private corporations yet always backed and permitted by the state. Private content platforms regulate online speech (Klonick 2018), as in the case of Facebook's independent content-moderation board (originally termed a "Supreme Court").[20] Similarly, the company's project to create a private, global digital currency—called the Libra—crucially depended on the backstopping mechanism offered by safe assets from reputable territorial sovereigns. But as Pistor (2020a) points out, the Libra association still aspired to operate beyond the reach of any national governmental regulation. Furthermore, Facebook's extraordinary control over users' personal data might still offer an alternative kind of backstopping, allowing the Libra to be unpegged from safe assets and function as private fiat currency: "If the option to monetize these data is sufficiently credible, the complete control over data may well substitute "the full faith and credit" of a legacy state." This raises "the specter of a statehood founded in data, not territory, or 'digital statehood'" (Pistor 2020a, 8), with controlling power in the hands of a small corporate elite, or a tech-savvy political elite (as in China).

In other words, it is important to recognize that the ultimate goal of digital innovations such as smart contracts and e-currencies is not to simply facilitate transactions, but to fully supplant forms of social regulation and economic control historically reserved for the sovereign (notwithstanding the fact that, in the realm of dispute resolution, private arbitration has already subsumed much of the state's role over recent decades). Conceived as sovereigns in their own right, platforms appear as totalizing institutions from which users have no realistic option of escaping (Pasquale 2015, 144; Klonick 2018, 1617 n125): traditional private-law protections, like terms-of-service agreements are wholly ineffective (Facebook famously dismantled its privacy protections after it destroyed the competition by selling itself as a privacy-conscious service [Srinivasan 2019]); and detailed information on users makes them more vulnerable to unfair practices, from monopolistic prices to statistical discrimination. In fact, rule by data may signal "the end of markets" (Pistor 2020b).

Meanwhile, the very conception of good governance promoted by the tech industry has cohered around corporate ideals such as customer service, responsiveness, and customization rather than, for example, equity or distributive justice. These values can be found in the writings of Tim O'Reilly, the Silicon Valley guru responsible for coining "Government 2.0" and "government as a platform;" in the work of "gov-tech" incubator Code for America; and in Cass Sunstein's (2013) reflections on his time

[19] This is obviously not new; the nullification of publicly recognized rights through claims of private sovereignty has a long history (for example, see Anderson 2017; Crouch 2011).

[20] Facebook. 2019. "Establishing Structure and Governance for an Independent Oversight Board." September 17, 2019. https://about.fb.com/news/2019/09/oversight-board-structure.

importing behavioral economics into the Obama-era Office of Information and Regulatory Affairs. In these accounts, the disruption of the state's operations by technological innovation is portrayed as a net benefit to the public, a source of economic opportunities, and a visionary claim on the future.

But inviting Silicon Valley into every realm of public life seems mainly to herald more commodification, stratification, and relentless competition. Some critics fear that "Silicon Valley companies are becoming 'shadow education ministries' (Selwyn 2016, 131) with the entrepreneurial capacity to set reformatory agendas for contemporary education" (Williamson 2017). AI-based educational platforms—one of them (Summit) partially bankrolled by Mark Zuckerberg—promise to break down the boundaries between school and home and deliver personalized learning, adapted to the individual needs of each child. Through collaborations with school districts, children are also forcibly enrolled into online platforms that transform them into data repositories ripe for extraction. As Deleuze anticipated, the relentlessness of capitalism matches up well with the kinds of affordances embedded in computing and digital technologies: "perpetual training tends to replace the school, and continuous control to replace the examination. Which is the surest way of delivering the school over to the corporation" (1992, 4). A similar logic, incidentally, may be unfolding in the prison system. As prisons shift basic services (such as visitation) to digital tools (e.g., video chat), or offer new services (e.g., online courses), not only are costs often transferred to prisoners and their families, but a captive, state-managed population is delivered wholesale to various data-collection (and thus commodification) purposes.[21]

The more the goals and means of public governance are outsourced to algorithms, and in turn to corporations, the more traditional vessels of collective purpose (such as collective action, or the law) will be delegitimated as obsolete or too (visibly) political. On this point, we are far from the first to express concern about the consequences of government outsourcing and public-private partnerships. Our more novel claim is that when the state defines itself as a statistical authority, an open data portal, or a provider of digital services, it opens itself up to competition from private alternatives that may command equal or greater legitimacy on these terms. This is in part because the state is generally not as adept at providing digital services as the firms that specialize in doing so, at least under current conditions. More fundamentally, the state's legal compunction to treat all citizens equally may disadvantage it against private competitors for whom ranking, stratification, and price discrimination are core tools of the trade.

These outcomes are not inevitable. In the Conclusion, we consider several approaches to reasserting sovereignty over the apparatus of surveillance capitalism and over state-like corporations.

IV. Conclusion: Seeing Like a Citizen

A torrent of recent commentary in Law and Political Economy has sought to uncover "public" purpose in areas of law and policy conventionally thought to govern relations between "private" actors (Fisk 2019; Zatz 2019; Purdy 2017). Operating on the same schematic, other authors have decried the erosion of public control over putatively public institutions and branches of law (Vaheesan 2019). A key implication of our analysis is that we should not assume that "public" has a fixed meaning across different paradigms of statecraft, nor that public and private are necessarily opposites. If, as we argue, the ascendant mode of statecraft relies on phenomenology and technology developed in the heart of surveillance capitalism, restoring ownership and legal authority to public bodies will only go so far. We urge scholars and reformers to pay attention not just to the legal boundaries between state and market (no doubt a crucial site of contestation), but also to the forms of knowledge and modes of apperception at work within the state itself.

[21] A recent report noted that "price-gouging in commissaries is concentrated in the digital realm" (Raher 2018).

Different modes of statecraft make different assumptions about what is to be governed, and how. The high modernist state is congenitally fearful that society (especially its remote and peripheral regions) is slipping out of control, overflowing its proper borders, and eluding the metropole's grasp. It deals with this problem by imposing borders, taking censuses, and coercing those on the outskirts of society into legibility. The neoliberal state, for its part, is most concerned about the sovereignty of its individual, entrepreneurial economic subjects. To live out their proper version of freedom, according to accounts such as Hayek's, economic subjects need the state to help build up and protect private markets and to guarantee competition, which nature cannot be counted on to provide. At least, the neoliberal state proffers this noble-sounding line to cover its second agenda of redistributing resources upward to corporations and the wealthy (Harvey 2007). And so, neoliberal governmentality entails building a world where, on the one hand, the poor and working class are forced to take responsibility for themselves and compete for rights and benefits that are indexed to success in a market, while, on the other hand, corporations and the wealthy are insulated from meaningful competition and given preferential access to the benefits and protections bestowed by the state.

The dataist state is in many ways less concrete about its aspirations (compared to the neoliberal state, which is fixated on economic growth) and its fears (compared to the high-modernist state, which is fixated on disorder). Instead, its sights hover over an expanse of emergent opportunities and threats. Its data-trawling must be universal and comprehensive precisely because these threats and opportunities may arise anywhere. A functional explanation of why the dataist state has emerged now might start from the observation that, weakened by decades of anti-government ideology and concomitantly eroded capacity, Western states have determined to manage social problems as they bubble up into crises rather than intervening in their causes. Meanwhile, erosion between public and private is most advanced in the global South, where multinational firms have imported the techniques of surveillance and digital administration developed elsewhere before state capacity had developed to claim these responsibilities as its own.

We have argued that seeing society as so many streams of data leads the state to identify goals and control opportunities through individualized and behaviorist lenses. But if deployed in a "high-modernist" manner, by mining new data sources opportunistically to provide solutions to technocratically imposed social goals, the only thing that may ensue is another high-modernist disaster. There is no practical guarantee that the hyper-rationalism of the coder-king, or even the inscrutable algorithm, will do better than that of the bureaucratic planner, no matter how well informed they both may be (Burrell and Fourcade 2020). As Ben Green (2010) rightly points out, the smart city conceived as a series of optimization problems fed with real-time sensor data may turn out to be just as unlivable as the high-modernist city. Similarly, whatever the surveillance state gains in control and efficiency from using machine learning may come at the cost of a big cultural and political loss for the mass of citizens. Fully stemming the tide of digital technology is probably unrealistic. But digital technologies need not be driven by the ideology of data solutionism. The question that must be asked, as always, is one of political organization: how might these technologies be governed in such a way that they better and more equitably serve the public?

Our argument is that the state must learn to see like a citizen. Seeing like a citizen is a mode of statecraft that identifies social problems—including those problems stemming from the deployment of dataism itself—from the perspective of those affected. By citizens, we do not mean only those people who enjoy formal legal citizenship. Instead, we have in mind Dewey's notion of the public: everyone directly or indirectly affected by some action (Dewey 1954). The stateless and those denied legal citizenship should often be counted as epistemological citizens by this definition.

Although not in exactly these terms, Law and Political Economy scholars have begun to emphasize the radical power of governing by empowering and surfacing the knowledge of those affected by public policy. Rahman and Gilman (2019) argue for infusing bureaucratic decision making with participation by non-experts, and Dwyer-Reynolds (2019) advocates calling on citizen panels, known as administrative juries, to make environmental regulatory decisions. These proposals do not require heroic assumptions about ordinary people's capabilities and wisdom. They rely on the Deweyan proposition that a group of people with a thoughtful protocol for aggregating their views (like a jury's) can achieve an "embodied intelligence" greater than the sum of its parts (Dewey 1954, 210). Digital technologies could help make such a protocol both inclusive and effective. For example, Morozov (2019) offers a series of innovative propositions to use "digital feedback infrastructures" to help citizens get their local problems onto a public agenda,[22] organize relatively decentralized government bureaucracies, and build public platforms for citizens to donate and sell products and services to each other, with production directed by citizens' expressed needs (Saros 2014).

Seeing like a citizen would also logically require asserting public oversight over the machinery of surveillance capitalism. The tech industry was one of the most highly concentrated in the United States before the COVID-19 pandemic.[23] This is partly due to the monopolistic tendencies (both natural and fabricated) of some digital technologies,[24] and partly due to a history of lenient antitrust enforcement (Cohen 2019; Khan 2019; Philippon 2019). Living outside the material infrastructure of the internet was already marginalizing, but the pandemic has made digital inclusion essential for everyone. To the extent that digital technologies already feel like public goods (Fourcade 2020), why don't we treat them that way? One solution, then, may be to fully reorganize basic digital infrastructures, where feasible, as public utilities rather than profit-seeking firms, and to de-commodify a number of essential internet-based services—including, possibly, search and social media (Morozov 2019; Malmgren 2017). Depending on the size, function, and type of power embodied by particular platform businesses, some may be suitable for public ownership, others for cooperative ownership, devolution to open-source non-ownership, or outright abolition (Tarnoff 2019).

But even beyond the question of ownership, public accountability over dataism requires a new understanding of algorithmic accountability (Pasquale 2019). In what Frank Pasquale calls the "first wave" of algorithmic accountability and what others have termed "data justice," scholars stressed the importance of providing the subjects of data analysis with the power to see into that analysis, the power to control (including to reject) their participation in data collection, and protection from biased or discriminatory analysis (Taylor 2017). Pasquale defines the "second wave" of algorithmic accountability as empowering citizens to challenge the basic existence of algorithms that rank and classify us, rather than (or in addition to) just reviewing them for bias. For example, Julia Powles and Helen Nissenbaum (2018, n.p.) ask: "Which systems really deserve to be built? Which problems most need to be tackled? Who is best placed to build them? And who decides? We need genuine accountability mechanisms, external to companies and accessible to populations." Where first-wave accountability sought to empower individuals to control the terms of their own surveillance, second-wave accountability suggests a more collective form of governance. This view of algorithmic accountability represents a meaningful alternative to the popular notion of protecting privacy by granting individual property rights in data. Rather than parting with data on the basis of price alone,

[22] See, for example, the digital 311 platform (Sisson 2017).

[23] There are many indications that concentrations levels have further increased since the pandemic began.

[24] As Evgeny Morozov explains, "[T]he more people on Facebook, the more valuable it becomes, and it doesn't really make sense to have five competing social networks with twenty million people on each; you want all of them on one platform. It's the same for search engines: the more people are using Google, the better it becomes, because every search is in some sense a tinkering and improvement in the service" (2015, n.p.) The first advantage is known as "network effects"; also see Stalder (2018, 143) on the connection between network effect and monopoly effect. The second is a direct consequence of the way cybernetic feedback/machine learning works.

second-wave accountability imagines Internet users, organized in deliberative groups, affirming or rejecting tracking systems based on their social effects—and deciding so for principled reasons, rather than the lure of a good price.

Seeing like a citizen might also mean not just democratizing the software that surveils and evaluates all of us, but turning that scrutiny back upon the state and politicians themselves. Democracy consists not only of amplifying the people's voice, but also magnifying the people's gaze as a form of discipline over potentially unaccountable leaders (Green 2010). Jeffrey Green's concept of "ocular democracy" acknowledges that many people are more comfortable participating in politics as spectators than as actors, but insists that even spectatorship, properly channeled, can advance democracy. The key is to assert the public's power over elites by establishing political *candor*, the requirement that leaders not control the conditions of their own publicity. Ocular democracy would require various reforms of media institutions through which citizens learn about the government. It might also involve a new conception of "open government," in which transparency means not just open access to innocuous traffic data but, for example, spontaneously televised meetings between politicians and lobbyists or access to the deliberations of surveillance bureaucrats at the NSA. The Edward Snowden leaks might be seen as a first step in creating the conditions for ocular democracy. In order for politicians and bureaucrats to change their behavior in response to the public's disciplinary gaze, however, such leaks would need to be regular occurrences. Moreover, private regulators and proxy sovereigns would need to be subjected to the same scrutiny.

Seeing like a citizen will generally lack the predictive capacity of seeing like a market—unless one means a prediction market, a device for aggregating many people's bets into supposedly accurate predictions. But seeing like a citizen will no doubt bring other advantages, including the ability to preserve certain values (see, for instance, the San Francisco ordinance banning the use of facial recognition) or to promote different kinds of information. Citizens know things; they each know things that no one else does. Social theorists have long debated how to make use of that local knowledge. It was once argued that prices were the only realistic way to convey local information across space and time (Hayek 1945). But this claim is contingent on the communication and information systems available. The data-analytic technologies currently favored by corporations and the state will only continue to grow more accurate in their predictions. Depending where one sits, this development will be some combination of useful and disturbing. But either way, a state whose unique methodologies are prediction and alignment is far from tapping the full potential of collective life.

Many scholars will warn that seeing like a citizen is a tall political order at this point. Felix Stalder, for instance, suggests that the digital condition is fundamentally "post-democratic": it degrades "the expectations that citizens have for democratic institutions, and it makes their increasing erosion seem . . . normal" (2018, 147). Yuval Harari's (2018) judgment is even bleaker: artificial intelligence, he argues, has both the potential to render a large swath of the population useless, and to process large amounts of information centrally. This makes authoritarian systems oriented to total surveillance much more efficient than democratic ones. Faced with these prophets of doom[25] and a very uncertain political present, our argument extolling the promise of citizen-originated solutions may sound like wishful thinking.

And yet, as we see it, the door is far from closed on democracy. Authoritarian surveillance is still in its early stages, for better or worse, and public backlash is ubiquitous, if inchoate. Given our view that the fundamental technologies of the digital age (distributed systems, machine learning) are not going anywhere, the question is whether we can put them to more solidaristic and less authoritarian use. There is no escape in Luddism. Therefore, the essential task for today's civic technologists is to build

[25] Other prescient forebears include Phil Agre (1994) and William Bogard (1996).

systems for incorporating each citizen's information and amplifying each citizen's voice, and doing so at the proper moments so those voices combine, not into the cacophony we have grown accustomed to, but into a coherent democratic chorus.

REFERENCES

Agamben, Giorgio. 1998. *Homo Sacer: Sovereign Power and Bare Life*. Stanford University Press.

Agamben, Giorgio. 2014. "For a Theory of Destituent Power." *Critical Legal Thinking* (blog), February 5, 2014. https://criticallegalthinking.com/2014/02/05/theory-destituent-power.

Agre, Philip E. 1994. "Surveillance and Capture: Two Models of Privacy." 10 *The Information Society* 101.

Ahmed, Shazeda. 2019. "The Messy Truth About Social Credit." *Logic Magazine*, May 1, 2019. https://logicmag.io/china/the-messy-truth-about-social-credit.

Alemanno, Alberto. 2018. "Data for Good: Unlocking Privately-Held Data to the Benefit of the Many." 9 *European Journal of Risk and Regulation* 2.

Amoore. Louise. 2009. "Lines of Sight: On the Visualization of Unknown Futures." 13 *Citizenship Studies* 17.

Amoore, Louise. 2013. *The Politics of Possibility*: *Risk and Security Beyond Probability*. Duke University Press.

Anderson, Elizabeth. 2017. *Private Government: How Employers Rule Our Lives (and Why We Don't Talk About It)*. Princeton University Press.

Andriotis, AnnaMaria. 2019. "New Trump Administration Rule Will Look at Immigrants' Credit Histories." *Wall Street Journal,* August 16, 2019. https://www.wsj.com/articles/new-trump-administration-rule-will-look-at-immigrants-credit-histories-11565973971.

Aradau, Claudia, and Rens Van Munster. 2007. "Governing Terrorism through Risk: Taking Precautions, (Un)knowing the Future." 13 *European Journal of International Relations* 89.

Aronova, Elena, Christine von Oertzen, and David Sepkoski. 2017. "Introduction: Historicizing Big Data." "Data Histories," special issue. 32 *Osiris 1*. https://www.journals.uchicago.edu/toc/osiris/2017/32/1.

Benjamin, Ruha. 2019. *Race After Technology. Abolitionist Tools for the New Jim Code*. Polity.

Birch, Kean. 2019. "Technoscience Rent: Toward a Theory of Rentiership for Technoscientific Capitalism." 45 *Science, Technology and Human Values* 3. https://doi.org/10.1177/0162243919829567.

Birch, Kean, and Fabian Muniesa, eds. 2020. *Assetization: Turning Things into Assets in Technoscientific Capitalism*. MIT Press.

Björklund, Fredrika. 2016. "E-Government and Moral Citizenship: The Case of Estonia." 20 *Citizenship Studies* 914.

Black, Edwin. 2001. *IBM and the Holocaust: The Strategic Alliance between Nazi Germany and America's Most Powerful Corporation.* Crown Books.

Bogard, William. 1996. *The Simulation of Surveillance: Hypercontrol in Telematic Societies.* Cambridge University Press.

Bouk, Dan. 2015. *How Our Days Became Numbered: Risk and the Rise of the Statistical Individual.* University of Chicago Press.

Bouissou, Julien. 2019. "Le big data bouleverse la prédiction économique." *Le Monde*, September 18, 2019. https://www.lemonde.fr/economie/article/2019/09/18/le-big-data-bouleverse-la-prediction-economique_5511835_3234.html#xtor=AL-32280270.

Bourdieu. Pierre. 2015. *On the State: Lectures at the Collège de France, 1989–1992.* Polity.

Brayne, Sarah. 2014. "Surveillance and System Avoidance: Criminal Justice Contact and Institutional Attachment." 79 *American Sociological Review* 866.

Brayne, Sarah. 2020. *Predict and Surveil: Data, Discretion, and the Future of Policing.* Oxford University Press.

Britton-Purdy, Jedediah S., David Grewal, Amy Kapcyznski, and K. Sabeel Rahman. 2020. "Building a Law and Political Economy Framework: Beyond the Twentieth-Century Synthesis." 129 *Yale Law Journal* 1784.

Brock, David C. 2018. "Learning from Artificial Intelligence's Previous Awakenings: The History of Expert Systems." 39 *AI Magazine* 3.

Brown, Wendy. 2015. *Undoing the Demos: Neoliberalism's Stealth Revolution.* Zone Books.

Buckley, Chris, and Paul Mozur. 2019. "How China Uses High-Tech Surveillance to Subdue Minorities." *New York Times*, May 22, 2019. https://www.nytimes.com/2019/05/22/world/asia/china-surveillance-xinjiang.html.

Bulusu, Siri. 2018. "Palantir Deal May Make IRS 'Big Brother-ish' While Chasing Cheats." *Bloomberg Law*, November 15, 2018. https://biglawbusiness.com/palantir-deal-may-make-irs-big-brother-ish-while-chasing-cheats.

Burrell, Jenna. 2016. "How the Machine Thinks: Understanding Opacity in Machine Learning Algorithms." 3 *Big Data and Society* 1. https://doi.org/10.1177/2053951715622512.

Burrell, Jenna, and Marion Fourcade. 2020. "The Society of Algorithms." Unpublished manuscript.

Cheney-Lippold, John. 2017. *We Are Data: Algorithms and the Making of Our Digital Selves.* NYU Press.

Cheung, Anne Shann Yue, and Chen, Yongxi Clement. 2018. "The Rise of the Data State: The Case of China's Social Credit System." Working paper in proceedings of "Emerging Technologies and the Future of Citizenship," June 2018, WZB Social Science Center, Berlin.

Christin, Angèle. 2017. "Algorithms in Practice: Comparing Web Journalism and Criminal Justice." 4 *Big Data & Society* 1. https://doi.org/10.1177/2053951717718855.

Citron, Danielle. 2008. "Technological Due Process." 85 *Washington University Law Review* 1249.

Citron, Danielle, and Ryan Calo. 2019. "Automation and the Crisis of Legitimacy in the Administrative State." Presented at the Privacy Law Scholars' Conference, May 30-31, 2019, UC Berkeley.

Coglianese, Cary, and David Lehr. 2017. "Regulating by Robot: Administrative Decision Making in the Machine-Learning Era." 105 *Georgetown Law Journal* 1147.

Cohen, Julie E. 2016. "The Regulatory State in the Information Age." 17 *Theoretical Inquiries in Law* 369.

Cohen, Julie E. 2018. "The Biopolitical Public Domain: The Legal Construction of the Surveillance Economy." 31 *Philosophy and Technology* 213.

Cohen, Julie E. 2019. *Between Truth and Power: The Legal Constructions of Informational Capitalism*. Oxford University Press.

Crouch, Colin. 2011. *The Strange Non-Death of Neoliberalism*. Polity Press.

Cuéllar, Mariano-Florentino. 2017. "Cyberdelegation and the Administrative State." In *Administrative Law from the Inside Out: Essays on Themes in the Work of Jerry L. Mashaw*, edited by Nicholas R. Parrillo, 134. Cambridge University Press.

Cuéllar, Mariano-Florentino, and Aziz Z. Huq. Forthcoming. "Privacy's Political Economy and the State of Machine Learning: An Essay in Honor of Stephen J. Schulhofer." *NYU Annual Survey of American Law.*

Deleuze, Gilles. 1992. "Postscript to the Societies of Control." 59 *October* 3.

Deleuze, Gilles, and Félix Guattari. 1987. *A Thousand Plateaus: Capitalism and Schizophrenia.* University of Minnesota Press.

Desrosières, Alain. 2002. *The Politics of Large Numbers. A History of Statistical* Reasoning. Harvard University Press.

Dewey, John. 1939. *Theory of Valuation*. In *The Later Works of John Dewey, 1925-1953,* vol. 13, edited by Jo Ann Boydston, 189. Southern Illinois Press.

Dewey, John. 1954 [1927]. *The Public and Its Problems*. Swallow Press.

Domingos, Pedro. 2015. *The Master Algorithm: How the Quest for the Ultimate Learning Machine Will Remake Our World*. Basic Books.

Dreyfus, Hubert, and Stuart Dreyfus. 2005. "Peripheral Vision: Expertise in Real World Contexts." 26 *Organization Studies* 779. https://doi.org/10.1177/0170840605053102.

Dwyer-Reynolds, Conor. "To Democratize Environmental Law, Let Ordinary People Decide." *Law and Political Economy (*blog), September 26, 2019. https://lpeblog.org/2019/09/26/to-democratize-environmental-law-let-ordinary-people-decide.

Engstrom, David, Daniel Ho, Catherine Sharkey, and Mariano-Florentino Cuéllar. 2020. *Government by Algorithm: Artificial Intelligence in Federal Administrative Agencies*. Report submitted to the Administrative Conference of the United States, February 2020. https://www-cdn.law.stanford.edu/wp-content/uploads/2020/02/ACUS-AI-Report.pdf.

Eubanks, Virginia. 2017. *Automating Inequality. How High-Tech Tools Profile, Police and Punish the Poor*. St Martin's Press.

Farrell, Henry. 2018. "Privatization as State Transformation." 60 *Nomos* 171.

Farrell, Henry. 2019. "Seeing Like a Finite State Machine." *Crooked Timber* (blog), November 25, 2019. http://crookedtimber.org/2019/11/25/seeing-like-a-finite-state-machine.

Fisk, Catherine L. 2019. "Rethinking Public and Private Power: Anderson's Private Government and Labor Law Reform." *Law and Political Economy* (blog), April 4, 2019. https://lpeblog.org/2019/04/04/rethinking-public-and-private-power-andersons-private-government-and-labor-law-reform.

Foucault, Michel. 1998. *History of Sexuality, vol. 1*. Penguin Books.

Foucault, Michel. 2010. *The Birth of Biopolitics: Lectures at the College de France, 1978-1979*. Palgrave MacMillan.

Fourcade, Marion. 2017. "The Fly and the Cookie: On the Moral Economy of 21st Century Capitalism." 15 *Socio-Economic Review* 661.

Fourcade, Marion. Forthcoming. "Ordinal Citizenship." *British Journal of Sociology*.

Fourcade, Marion, and Kieran Healy. 2017a. "Seeing Like a Market." 15 *Socio-Economic Review* 9.

Fourcade, Marion, and Kieran Healy. 2017b. "Categories All the Way Down." 42 *Historical Social Research* 286.

Fourcade, Marion, and Fleur Johns. Forthcoming. "Machine-Learnable Society: Experience, Structure, Politics." *Theory & Society*.

Fourcade, Marion, and Daniel N. Kluttz. 2020. "A Maussian Bargain: Accumulation by Gift in the Digital Economy." 7 *Big Data & Society* 1. https://doi.org/10.1177/2053951719897092.

Fry, Hannah. 2018. *Hello World: Being Human in the Age of Algorithms*. W. W. Norton & Company.

Galloway, Alexander. 2004. *Protocol: How Control Exists After Decentralization*. MIT Press.

Gandy, Oscar Jr. 1993. *The Panoptic Sort: A Political Economy of Personal Information*. Westview Press.

Giridharadas, Anand. 2018. *Winners Take All: The Elite Charade at Changing the World*. Knopf.

Goodman, Ellen P., and Julia Powles. 2019. "Urbanism under Google: Lessons from Sidewalk Toronto." 88 *Fordham Law Review* 457.

Gray, Mary, and Siddarth Suri. 2019. *Ghost Work: How to Stop Silicon Valley from Building a New Global Underclass.* Houghton Mifflin Harcourt.

Green, Jeffrey Edward. 2010. *The Eyes of the People: Democracy in an Age of Spectatorship.* Oxford University Press.

Hacker, Jacob. 2002. *The Divided Welfare State: The Battle Over Public and Private Social Benefits in the United States.* Cambridge University Press.

Harari, Yuval Noah. 2017. *Homo Deus: A Brief History of Tomorrow.* HarperCollins.

Harari, Yuval Noah. 2018. "Why Technology Favors Tyranny." *Atlantic Monthly*, October 2018. https://www.theatlantic.com/magazine/archive/2018/10/yuval-noah-harari-technology-tyranny/568330.

Harcourt, Bernard. 2008. *Against Prediction: Profiling, Policing, and Punishing in an Actuarial Age.* University of Chicago Press.

Harcourt, Bernard. 2015. *Exposed: Desire and Disobedience in the Digital Age.* Harvard University Press.

Harvey, David. 2007. "Neoliberalism as Creative Destruction." 610 *Annals of the American Academy of Political and Social Science* 21.

Hayek, Friedrich A. von. 1945. "The Use of Knowledge in Society." 35 *American Economic Review* 519.

Ho, Ezra. 2017. "Smart Subjects for a Smart Nation? Governing (Smart) Mentalities in Singapore." 54 *Urban Studies* 3101. https://doi.org/10.1177/0042098016664305.

Huq, Aziz Z. 2020. "A Right to a Human Decision." 106 *Virginia Law Review* 611.

Johns, Fleur. 2017. "Data, Detection, and the Redistribution of the Sensible in International Law." 111 *American Journal of International Law* 57.

Johns, Fleur. 2019. "From Planning to Prototypes: New Ways of Seeing Like a State." 82 *Modern Law Review* 833.

Kellogg, Kate, Melissa Valentine, and Angèle Christin. 2020. "Algorithms at Work: The New Contested Terrain of Control." 14 *Academy of Management Annals* 366.

Khan, Lina. 2019. "The End of Antitrust History Revisited." 133 *Harvard Law Review* 1655.

Khera, Reetika. 2019. "Aadhaar: Uniquely Indian Dystopia?" 21 *European Economic Sociology Newsletter,* November 24, 2019. https://econsoc.mpifg.de/38371/02_Khera_Econsoc-NL_21-1_Nov2019.pdf.

Klonick, Kate. 2018. "The New Governors: The People, Rules, and Processes Governing Online Speech." 131 *Harvard Law Review* 1598.

Kroll, Joshua, Solon Barocas, Ed Felten, Joel Reidenberg, David Robinson, and Harlan Yu. 2017. "Accountable Algorithms." 165 *University of Pennsylvania Law Review* 633.

Lakoff, Andrew. 2007. "Preparing for the Next Emergency." 19 *Public Culture* 247.

Lauer, Josh. 2017. *Creditworthy: A History of Consumer Surveillance and Financial Identity in America.* Columbia University Press.

Lessig, Lawrence. 1999. "The Law of the Horse: What Cyberlaw Might Teach." 113 *Harvard Law Review* 501.

Lewis, Michael. 2018. *The Fifth Risk*. W. W. Norton & Company.

Liu, H-W., Lin, C-F., and Chen, Y-J. 2019. "Beyond *State v Loomis*: Artificial Intelligence, Government Algorithmization and Accountability." 27 *International Journal of Law and Information Technology* 122.

Loubère, Nicholas. 2017. "L'essor de la finance sur Internet en Chine et les tyrannies de l'inclusion." 4 *Perspectives Chinoises* 11. http://journals.openedition.org/perspectiveschinoises/7886.

Malmgren, Evan. 2017. "The New Sewer Socialists." *Logic* (blog), December 1, 2017. https://logicmag.io/justice/the-new-sewer-socialists.

Matsakis, Louise. 2019. "How the West Got China's Social Credit System Wrong." *Wired,* July 29, 2019. https://www.wired.com/story/china-credit-score-system.

Mazzucato, Mariana. 2013. *The Entrepreneurial State: Debunking Public vs. Private Sector Myths*. Anthem.

Mehrling, Perry. "The Inherent Hierarchy of Money." January 25, 2012. Paper prepared for Duncan Foley festschrift volume and conference, April 20-21, 2012. https://ieor.columbia.edu/files/seasdepts/industrial-engineering-operations-research/pdf-files/Mehrling_P_FESeminar_Sp12-02.pdf.

Mill, Stuart. 2020. "Who Owns the Future? Data Trusts, Data Commons, and the Future of Data Ownership." Future Economies Research and Policy Paper #7, Manchester Metropolitan University, January 2020. https://www.mmu.ac.uk/media/mmuacuk/content/documents/business-school/future-economies/mills-2020.pdf.

Morozov, Evgeny. 2014a. "The Rise of Data and the Death of Politics." *Technology* (blog), *The Observer,* July 19, 2014. https://www.theguardian.com/technology/2014/jul/20/rise-of-data-death-of-politics-evgeny-morozov-algorithmic-regulation.

Morozov, Evgeny. 2014b. *To Save Everything, Click Here: The Folly of Technological Solutionism*. Public Affairs Books.

Morozov, Evgeny. 2015. "Socialize the Data Centres!" 91 *New Left Review,* January-February 2015. https://newleftreview.org/issues/ll91/articles/evgeny-morozov-socialize-the-data-centres.

Morozov, Evgeny. 2019. "Digital Socialism? The Calculation Debate in the Age of Big Data." 116 *New Left Review,* March-June 2019. https://newleftreview.org/issues/ll116/articles/evgeny-morozov-digital-socialism.

Mozur, Paul, Jonah Kessel, and Melissa Chan. 2019. "Made in China, Exported to the World: The Surveillance State." *New York Times*, April 24, 2019. https://www.nytimes.com/2019/04/24/technology/ecuador-surveillance-cameras-police-government.html.

Narayanan, Arvind. 2019. "How to Recognize AI Snake Oil: 2019 Arthur Miller Lecture on Science and Ethics." Massachusetts Institute of Technology, November 18. Slides available at https://www.cs.princeton.edu/~arvindn/talks/MIT-STS-AI-snakeoil.pdf.

Noble, Safiya Umoja. 2018. *Algorithms of Oppression: How Search Engines Reinforce Racism*. NYU Press.

Obermeyer, Ziad, Brian Powers, Christine Vogeli, and Sendhil Mullainathan. 2019. "Dissecting Racial Bias in an Algorithm Used to Manage the Health of Populations." 366 *Science* 447. https://doi.org/10.1126/science.aax2342.

O'Mara, Margaret. 2019. *The Code: Silicon Valley and the Remaking of America*. Penguin Press.

O'Neil, Cathy. 2016. *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*. Broadway Books.

Pasquale, Frank. 2015. *The Black Box Society*. Harvard University Press.

Pasquale, Frank. 2018. "A Rule of Persons, Not Machines: The Limits of Legal Automation." University of Maryland Francis King Carey School of Law Legal Studies Research Paper No. 2018-08. https://digitalcommons.law.umaryland.edu/fac_pubs/1612.

Pasquale, Frank. 2019. "The Second Wave of Algorithmic Accountability." *Law and Political Economy* (blog), November 25, 2019. https://lpeblog/org/2019/11/25/the-second-wave-of-algorithmic-accountability.

Pear, Robert. 2019. "On Disability and on Facebook? Uncle Sam Wants to Watch What You Post." *New York Times*, March 10, 2019. https://www.nytimes.com/2019/03/10/us/politics/social-security-disability-trump-facebook.html.

Peck, Jamie. 2010. *Constructions of Neoliberal Reason*. Oxford University Press.

Philippon, Thomas. 2019. *The Great Reversal: How America Gave Up on Free Markets*. Belknap Press/Harvard University Press.

Pistor, Katharina. 2020a. "Statehood in the Digital Age." 27 *Constellations* 3.

Pistor, Katharina. 2020b. "Rule by Data: The End of Markets?" 83 *Law & Contemporary Problems* 101.

Porter, Theodore. 1996. *Trust in Numbers: The Pursuit of Objectivity in Science and Public Life*. Princeton University Press.

Powles, Julia, and Helen Nissenbaum. 2018. "The Seductive Diversion of 'Solving' Bias in Artificial Intelligence." *OneZero*, December 7, 2018. https://onezero.medium.com/the-seductive-diversion-of-solving-bias-in-artificial-intelligence-89Odf5e5ef53.

Prasad, Monica. 2018. *Starving the Beast: Ronald Reagan and the Tax Cut Revolution*. Russell Sage.

Purdy, Jedediah. 2017. "Understanding Environmental Law as Public Provision." *Law and Political Economy* (blog), November 29, 2017. https://lpeblog.org/2017/11/29/understanding-environmental-law-as-public-provision.

Qiang, Xiao. 2019. "The Road to Digital Unfreedom: President Xi's Surveillance State." 30 *Journal of Democracy* 53.

Raher, Stephen. 2018. "The Company Store: A Deeper Look at Prison Commissaries." https://www.prisonpolicy.org/reports/commissary.html.

Rahman, K. Sabeel, and Hollie Russon Gilman. 2019. *Civic Power: Rebuilding American Democracy in an Era of Crisis.* Cambridge University Press.

Rao, Ursula. 2019. "Biometric IDs and the Remaking of the Indian (Welfare) State." 21 *European Economic Sociology Newsletter,* November 2019. https://econsoc.mpifg.de/29175/econ_soc_21-1.pdf.

Raso, Jennifer. 2017. "Displacement as Regulation: New Regulatory Technologies and Front-Line Decision-Making in Ontario Works." 32 *Canadian Journal of Law and Society* 75.

Ricks, Morgan. 2016. "Entry Restriction, Shadow Banking, and the Structure of Monetary Institutions." 2 *Journal of Financial Regulation* 291.

Ries, Eric. 2011. *The Lean Startup: How Today's Entrepreneurs Use Continuous Innovation to Create Radically Sucessful Businesses*. Crown Publishing.

Robinson, David. 2018. "The Challenges of Prediction: Lessons from Criminal Justice." 14 *I/S: A Journal of Law and Policy for the Informational Society* 151.

Rose, Nikolas, and Mariana Valverde. 1998. "Governed by Law?" 7 *Social & Legal Studies* 541.

Sadilek, Adam, Stephanie Caty, Lauren DiPrete, Raed Mansour, Tom Schenk Jr, Mark Bergtholdt, Ashish Jha, Prem Ramaswami, and Evgeniy Gabrilovich. 2018. "Machine-Learned Epidemiology: Real-Time Detection of Foodborne Illness at Scale." 1 *npj Digital Medicine.* https://doi.org/10.1038/s41746-018-0045-1.

Sadowski, Jathan. 2020. *Too Smart: How Digital Capitalism is Extracting Data, Controlling our Lives, and Taking Over the World.* MIT Press.

Said, Carolyn. 2019. "Uber Must Share Data with San Francisco, Appeals Court Rules." *San Francisco Chronicle*, May 20, 2019. https://www.sfchronicle.com/business/article/Uber-must-share-data-with-San-Francisco-appeals-13864909.php.

Saros, Daniel. 2014. *Information Technology and Socialist Construction: The End of Capitalism and the Transition to Socialism*. Routledge.

Schick, Allen. 1970. "The Cybernetic State." 7 *Trans-Action* 13.

Scott, James. 1999. *Seeing Like a State: How Certain Schemes to Improve the Human Condition Have Failed.* Yale University Press.

Selwyn, Neil. 2016. *Is Technology Good for Education?* Polity.

Shapiro, Isaac. 2017. "Federal Employment at Record Lows as a Share of Employment Population." Center on Budget and Policy Priorities. Accessed September 28, 2020. https://www.cbpp.org/research/federal-budget/federal-employment-at-record-lows-as-a-share-of-employment-populationyet.

SeeClickFix. Patrick Sisson. 2017. "How a Simple App Can Actually Empower Street-Level Democracy," *Curbed* (blog), February 7, 2017. https://www.curbed.com/2017/2/7/14541760/311-app-digital-citizen-seeclickfix-digital-democracy.

Srinivasan, Dina. 2019. "The Antitrust Case against Facebook: Monopolist's Journey Towards Pervasive Surveillance in Spite of Consumers' Preference for Privacy." 16 *Berkeley Business Law Journal* 39.

Stalder, Felix. 2018. *The Digital Condition*. Polity.

Sunstein, Cass. 2013. *Simpler: The Future of Government.* Simon & Schuster.

Sunstein, Cass. 2015. "The Ethics of Nudging." 32 *Yale Journal on Regulation* 413.

Tarnoff, Ben. 2019. "Platforms Don't Exist." *Metal Machine Music*, November 22, 2019. https://bentarnoff.substack.com/p/platforms-dont-exist.

Taylor, Linnet. 2017. "What is Data Justice? The Case for Connecting Digital Rights and Freedoms Globally." 4 *Big Data & Society*. https://doi.org/10.1177/2053951717736335.

Taylor, Linnet, and Dennis Broeders. 2015. "In the Name of Development: Power, Profit and the Datafication of the Global South." 64 *Geoforum* 229.

Vaheesan, Sandeep. 2019. "The Erosion of Public Control Over Public Utilities." *Law and Political Economy* (blog), March 14, 2019. https://lpeblog.org/2019/03/14/the-erosion-of-public-control-over-public-utilities.

Valverde, Mariana, Fleur Johns, and Jennifer Raso. 2018. "Governing Infrastructure in the Age of the 'Art of the Deal': Logics of Governance and Scales of Visibility." 41 *Political and Legal Anthropology Review* 118.

Weber, Max. 1946. "Science as a Vocation." In *From Max Weber: Essays in Sociology*, edited and translated by H.H. Gerth and C.W. Mills, 129. Oxford University Press.

Walker, Amy. 2019. "NHS Gives Amazon Free Use of Health Data under Alexa Advice Deal." *Guardian,* December 8, 2019. https://www.theguardian.com/society/2019/dec/08/nhs-gives-amazon-free-use-of-health-data-under-alexa-advice-deal.

Wilcox, Scarlet. 2014. "Official Discourses of the Australian 'Welfare Cheat.'" 26 *Current Issues in Criminal Justice* 177.

Williamson, Ben. 2017. "Educating Silicon Valley: Corporate Education Reform and the Reproduction of the Techno-Economic Revolution."39 *Review of Education, Pedagogy, and Cultural Studies* 265. https://doi.org/10.1080/10714413.2017.1326274.

Wray, L. Randall. 2014. "What Are Taxes For? The MMT Approach." *New Economic Perspectives* (blog), May 15, 2014. https://neweconomicperspectives.org/2014/05/taxes-mmt-approach.html.

Yang, Yuan, and Nian Liu. 2019. "Alibaba and Tencent Refuse to Hand Loans Data to Beijing." *Financial Times*, September 18, 2019. https://www.ft.com/content/93451b98-da12-11e9-8f9b-77216ebe1f17.

Yu, Harlan, and David G. Robinson. 2012. "The New Ambiguity of 'Open Government.'" 59 UCLA *Law Review Discourse* 178.

Zatz, Noah. 2019. "The Public Law of Private Promising, and Not Even That: LPE 101 for Contracts." *Law and Political Economy* (blog), February 26, 2019. https://lpeblog.org/2019/02/26/the-public-law-of-private-promising-and-not-even-that-lpe-101-for-contracts.

Zuboff, Shoshana. 2019. *The Age of Surveillance Capitalism. The Fight for a Human Future at the New Frontier of Power.* Public Affairs.