DOI: 10.1111/lapo.12164

ORIGINAL ARTICLE

LAW & POLICY UNIVERSITY OF DENVER WILEY

The law in computation: What machine learning, artificial intelligence, and big data mean for law and society scholarship

Tania DoCarmo[1] | **Stephen Rea**[2] | **Evan Conaway**[3] | **John Emery**[4] | **Noopur Raval**[5]

[1]Legal Studies, University of Massachusetts Amherst, Amherst, Massachusetts, USA

[2]Humanities, Arts and Social Sciences, Colorado School of Mines, Golden, Colorado, USA

[3]Center for International Security and Cooperation, Stanford University, Stanford, California, USA

[4]Department of Anthropology, University of California Irvine, Irvine, California, USA

[5]AINow Institute, New York University, New York, New York, USA

Correspondence
Tania DoCarmo, Legal Studies, University of Massachusetts Amherst, 200 Hicks Way, Amherst, MA 01003, USA.
Email: tdocarmo@umass.edu

Funding information
National Science Foundation, Grant/Award Number: 1724735

Abstract

Computational systems, including machine learning, artificial intelligence, and big data analytics, are not only inescapable parts of social life but are also reshaping the contours of law and legal practice. We propose turning more law and social science (LSS) attention to new technological developments through the study of "law in computation," that is, computational systems' integration with regulatory and administrative procedures, the sociotechnical infrastructures that support them, and their impact on how individuals and populations are interpellated through the law. We present a range of cases in three areas of inquiry - algorithmic governance, jurisdiction and agency - on issues such as immigration enforcement, data sovereignty, algorithmic warfare, biometric identity regimes, and gig economies, for which examining law in computation illuminates how new technological systems' integration with legal processes pushes the distinction between "law on the books" and "law in action" into new domains. We then propose future directions and methods for research. As computational systems become ever more sophisticated, understanding the law in computation is critical not only for LSS scholarship, but also for everyday civics.

1 | INTRODUCTION

We read almost daily about the actual and potential impacts of artificial intelligence (AI) on society, from the conveniences of driverless cars and smart home appliances to concerns about worker displacement and new forms of surveillance. The machine learning (ML) and data analytics techniques that support AI systems already saturate our online activities, our homes, and our cities, even if we are not always aware of them. At the same time, controversies over new computational techniques' predictive value for everything from criminal justice decision-making to credit scoring are erupting in policy and advocacy circles.

Scholarly attention to these phenomena is too often siloed within science and technology studies, computer science, or law and technology discussions among legal professionals at law schools. They are only beginning to be discussed in the mainstream law and social science (LSS) literature, primarily focusing on changes in criminal law and procedure, with less emphasis on other topics. A survey of the three long-standing American journals that primarily publish empirical sociolegal scholarship shows only scant attention so far (see Figure 1). Of the fifty-five articles that include the terms "artificial intelligence," "machine learning," or "algorithm," only nine treat these computational phenomena as objects of analysis rather than as methodological tools. These articles consider topics such as computer vision and its implications for law and policy (Aronson, 2018; Brayne et al., 2018), predictive policing (Brayne, 2017), and the implications of computer animation and virtual environments for courtroom decision-making (Bailensen et al., 2006; Dunn et al., 2006).

Given how computational systems—the general term we use for AI, ML, data analytics, biometrics, Internet of Things, blockchain, mobile and cloud-based computing, biometrics, and algorithms—are not only inescapable parts of social life but also increasingly at issue in legal practice and processes, we argue that LSS scholars are well positioned to critically investigate these systems in unique ways and should pay more attention to these topics than they currently do. In other words, critical LSS scholarship on how the law works when it is integrated into new computational systems is currently too limited.

A generation ago, LSS scholars outlined a new paradigm for legal scholarship, focusing on social, economic, and political variables in the interpretation and execution of the law (see Abel, 2010). If the problem that they sought to address necessitated a paradigm shift from "the law on the books" to "the law in action" (Abel, 2010), we suggest that the integration of AI, ML, and big data with contemporary matters of governance necessitates another paradigm shift, this time to what we are calling "the law in computation." The time is ripe to consider the

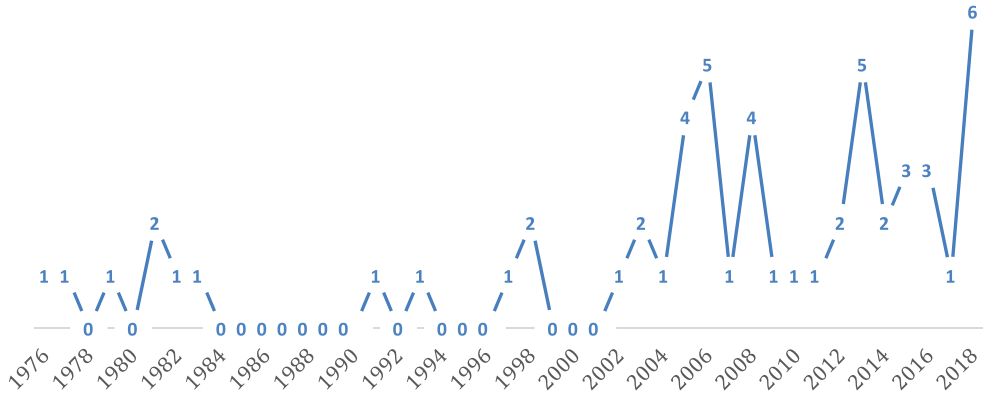

FIGURE 1 References to the terms "artificial intelligence," "machine learning," or "algorithm" in *Law & Policy*, *Law & Society Review*, and *Law & Social Inquiry*. Data: Wiley Online Library, journal articles only

following: how legal terrain is being created through new technologies; the evidentiary implications of innovative forms of knowledge and record-keeping; the legal forms that are being brought into being as legal actors adapt technologies to their own uses; and the insertion into the law of new computational agents programmed to make ethical decisions, comply with the law, or even make the law.

The law in computation encapsulates two related yet distinct developments: the availability and use of (often automated) computational systems in legal services for tasks such as "predictive coding" and "technology-assisted review" (Kluttz & Mulligan, 2019); and the proliferation of big data combined with AI- and ML-enabled technologies in adjudication and other decision-making processes, from risk assessment in criminal justice systems to public benefits disbursement in governmental agencies. While much has been written about technological transformations in law practices (Semmler & Rose, 2017; Surden, 2014), especially with respect to labor displacement (Katz, 2013; McGinnis & Pearce, 2014; Remus & Levy, 2017), our concern here is with computational systems' integration with big data, regulatory and administrative procedures, and the sociotechnical infrastructure that supports these procedures, as well as the impact of these computational systems on how individuals and populations are interpellated through the law.

Our collaboration grew out of a US National Science Foundation-funded project that brought together a diverse group of scholars from legal studies, social science, and information sciences to discuss the challenge of critically examining the proliferation of computational systems in social, economic, and political contexts around the world. This collaboration allowed us to see connections among our individual disciplines and projects, and to offer other LSS scholars avenues for beginning to delve into the law in computation, building on well-established LSS literature studies and establishing new ones.

To this end, we raise two conceptual areas in this paper that are crucial for a law-in-computation analytical framework: jurisdiction and legal agency. These are, of course, time-worn concepts in legal scholarship, but the law in computation raises new questions about them to which LSS scholars could undoubtedly offer unique contributions. To demonstrate some of the topics and debates in the area of the law in computation that warrant more scrutiny from LSS scholars, we present examples and case studies based on our own archival, ethnographic, and legal research that illuminate how computational systems' integration with legal processes pushes the distinction between "law on the books" and "law in action" into new domains. These case studies concern a range of topics, including the legal ramifications of cloud servers for data topographies, sovereignty, and localization; the ethics of algorithmic warfare; biometric and digital legal identity regimes' implications for surveillance, governance strategies, and contemporary legal personhood; the unsettled legal statuses of workers in gig economies; and the algorithmic management of labor. Each case raises critical issues for the law-in-computation approach, such as how legal frameworks for data management shape interventions in actual-world jurisdictions; how digital legal identities that are co-created with biometric technology, big data tools, and algorithmic processes affect legal subjectivities; and how technology-driven mechanisms impact individuals' and groups' legal status and agency (Table 1).

Our account is both descriptive and prescriptive. We present cases that intertwine law, society, and computational systems both to illustrate the contemporary terrain of sociolegal inquiry and to offer analytical recommendations for LSS scholars who encounter or seek out AI, ML, big data, and related computational systems in their work. Our work has also benefited from ongoing conversations with data activists and industry professionals in a variety of domains (e.g., fairness in credit scoring, immigrants' and labor rights activism, etc.). De-siloing our own research has entailed, for us, reaching into each other's citation circles as well as building bridges between computer science and sociolegal studies. We offer this article as a prolegomenon and set of guideposts for future LSS research.

TABLE 1 Areas of inquiry and case studies roadmap

Area of inquiry	Topic(s) explored	Examples and case studies
Algorithmic governance	Computational systems for outsourcing decision-making authority in public and private organizations	• Medicaid in Arkansas • Immigration enforcement (ICE) in New York
Jurisdiction	Data topographies, smart cities, data sovereignty, data localization	• Smart cities/LinkNYC • Predictive policing/PredPol • 2018 CLOUD Act • LiveJournal in Russia • Drones/lethal autonomous weapons (LAWS)
Agency	Actuarial subjects, biometric and digital identities/citizenship, virtual work, algorithmic labor	• Credit scoring • Aadhaar in India • ID2020 digital identity regime • Platform/gig economies

2 | ALGORITHMIC GOVERNANCE: PROMISES AND PITFALLS

At the turn of the twenty-first century, Lessig (2006), the prominent legal academic, internet activist, and founder of Creative Commons licensing, argued that computer code was usurping the place of law and regulation in structuring social and economic life. Code, he foresaw, would determine privacy, access, property, and speech—indeed, all that most liberal democratic societies had heretofore sought to regulate through law. His words were prescient. In fact, he may have underestimated the significance of the moment. If the situation Lessig described was one in which "code is law," in the decades since, advances in computational systems' capacity for enforcing rules a priori has ushered in an era in which the "law is code" (Hassan & De Filippi, 2017, p. 89). As we write, immigration vetting protocols use algorithmic assessments for prescreening (Hu, 2017), criminal sentences are being adjudicated based on analytics designed to predict criminal recidivism (Starr, 2014), and ML algorithms are being used to identify cybercrime supply chains from user activity in online forums (Bhalerao et al., 2019).

Such integrations of code with law reflect a broader shift in adjudication and regulation[1] toward *algorithmic governance*, that is, the "willingness to outsource decision-making authority to algorithm-based decision-making systems" (Danaher et al., 2017, p. 2). Algorithmic governance is made possible by the increasing number of ways to create and record data, including point of sale transactions, web searches, social media, and mobile telecommunications traffic, which allow for greater concentration of computing power, acceleration of processing speeds, and the potential to overcome humans' inability to analyze massive datasets quickly and at scale. ML algorithms' advantages in this context are their ability to identify nonintuitive correlations in big data that can be used to predict future behavior and their ability to learn from new data inputs and iteratively refine their models. Proponents of algorithmic governance point to improvements in operational efficiency and predictive accuracy resulting from the use of automated decision-making systems. For example, sensors throughout Los Angeles collect traffic data that are then analyzed in real time by an ML system, which automatically generates "rules" for the city's traffic signals (i.e., whether to stop a driver approaching an intersection or allow them to proceed) designed to reduce congestion (Coglianese & Lehr, 2019). Other proponents claim that algorithmic systems provide greater accountability, possibly eliminating the potential for corruption and discrimination (see Marx, 1995).

In theory, algorithmic governance tools can be used to improve efficiency, accuracy, and fairness by removing human biases from decision-making. Since an algorithm is not beholden to the same prejudices as human beings, so the argument goes, it can produce purely data-driven outcomes in the service of standardized, formalized rules for decision-making. A racist

police officer, for example, cannot simply arrest any Black male but must confirm a suspect's identity using facial recognition software. Following from this, algorithmic governance aligns well with the legal principle of due process because "consistently rendered decisions, on the basis of articulable and fixed criteria, are the hallmark of the kind of fairness that due process attempts to ensure" (Barocas et al., 2013, p. 9).

However, algorithms do not operate in a vacuum. An algorithm's accuracy can only be established relative to how it was programmed and the initial input that it was given (see Desai & Kroll, 2017). Moreover, algorithm-based automated decision makers are always embedded in the social contexts with which they are integrated and can inherit structural inequalities encoded in so-called "dirty data" such as historical records of policing (Richardson et al., 2019). Biases can also emerge from choices about feature selection and labeling when building ML models, all of which may surface some data at the expense of others and produce radically different outcomes, often with no opportunity for appeal. Facial-recognition analysis programs created by major technology companies, often used to help investigate criminal cases, for example, have demonstrated skin-type and gender biases. Built on original datasets of primarily White men, at least three such programs were recently unable to recognize the gender of darker-skinned women at error rates as high as 34% (Buolamwini & Gebru, 2018). In other words, algorithmic governance techniques may meet standards for procedural fairness while simultaneously "reproduc[ing] existing patterns of discrimination, inherit[ing] the prejudice of prior decision makers, or simply reflect[ing] the widespread biases that persist in society" (Barocas & Selbst, 2016, p. 674). Big data and the algorithms used to process it are by no means "infallible science" (Desai & Kroll, 2017, p. 4).

In addition to problems with fairness and bias, inconsistent regulations about how data are collected, shared, stored, and used affect automated decision makers' operations in different national, regional, and local jurisdictions. In particular, questions concerning government surveillance, informed consent, and privacy rights are germane to discussions of the degree to which individuals are aware that they are generating data through their activities, or how those data may be used. In any given context, jurisdictional differences in norms, rules, and regulations for data collection and their use trickle down to the micromechanics of the law in computation, producing a wide range of effects. For instance, revelations that Clearview AI—a facial recognition software company that works closely with law enforcement agencies in North America—had scraped images from social media websites including Facebook and YouTube without individual subscribers' knowledge or permission prompted a lawsuit from the state of Vermont's Attorney General alleging that the company had violated the state's consumer protection and data brokering laws (Cameron, 2020).[2]

Even if an organization informs individuals that it is collecting data about them, opting out of collection is not always possible. Moreover, privacy protections that apply to identifiable personal data in one place do not necessarily apply to the places where those data "live"—that is, to database servers' actual-world locations.[3] These regulatory divergences afford public and private institutions alike with opportunities to circumvent rules about data that they deem too restrictive. The "data arbitrage" practices used by these institutions demonstrate the real and potential gaps between jurisdictional theory and the technological capacity of computational systems in the era of big data. Thus, the data practices that make algorithmic governance possible make rethinking legal definitions of privacy, property, and agency all the more urgent.

Informed consent and awareness in data collection are part of broader concerns about the transparency (or lack thereof) of algorithmic governance's tools and mechanisms. Algorithms are often "black boxed" because of internal complexities, proprietary claims to their design and implementation, or both. But confronting these obstacles to transparency is not simply a matter of mandating that the underlying code or the model be made openly accessible. With respect to the inherent difficulty of making sense of why, exactly, algorithms—especially ML algorithms—perform the way that they do, "we concede that the algorithm's logic may not be

available to us—not because it's concealed, but because it's entirely beyond our view" (Barocas et al., 2013, p. 3). Limits to understanding how algorithms work not only present methodological problems for studying them and scrutinizing their impact but also make it harder to identify problems in algorithmic processing or to determine accountability when algorithms make harmful decisions (see Burrell, 2016; Dourish, 2016; Eubanks, 2017; Pasquale, 2015).

Improving transparency in algorithmic governance is often framed as a matter of *explainability*, that is, being able to clearly and reliably trace automated decision-making processes from the data collection stage, to running those data through a model, to determining how influential a particular input was on the model's outcome (Doshi-Velez et al., 2017). However, explanations are only meaningful insofar as they are *legible*—that is, understandable within the specific contexts in which a decision has been rendered and by the people who are most affected by it (Coldicutt, 2018). For example, in 2016, the state of Arkansas integrated an algorithmic assessment tool into its system for allocating home care visits covered by Medicaid, which led to drastic reductions in the number of hours that patients were allotted by the automated decision maker. The state's health care workers who administered the assessments could not explain why the algorithm had produced the decisions that it did, and limitations on understanding how it worked made it more difficult for patients to challenge those decisions and seek legal recourse. Legal Aid of Arkansas sued the state in federal court on the grounds that integrating the assessment tool without prior notification was a violation of procedural fairness, and as part of the suit it submitted a Freedom of Information Act (FOIA) request to review the algorithm and identify the key variables that determined its outcomes. Ultimately, Arkansas's use of the algorithm was ruled unconstitutional, but the damage, in many cases, had already been done (Lecher, 2018).

Recently, the New York Civil Liberties Union and Bronx Defenders filed a lawsuit against a New York field office of Immigration and Customs Enforcement (ICE) for manipulating its "Risk Classification Assessment Tool" algorithm, which determines whether individuals should be let go or detained based on their risk scores. The FOIA data analyzed in the lawsuit show that between 2013 and 2017, "the algorithm recommended detention without bond for 'low risk' individuals 53 percent of the time" (Biddle, 2020). But from June 2017 to September 2019, that number jumped to 97%, accompanied by a large uptick in ICE arrests under the Trump presidency. The algorithm is supposed to provide a recommendation to ICE officers who are then meant to make the final decision. Since 2017, the ICE field office in New York have followed the algorithm's recommendation over 99% of the time; however, when their cases were reviewed by immigration judges, roughly 40% of detainees were granted release on bond (Biddle, 2020). This suggests that ICE justifies existing practices by outsourcing decision-making to the ML algorithm, exacerbating patterns of discrimination that do not hold up to human judicial scrutiny. Moreover, during the time it took to process FOIA requests, mass detentions and deportations took place under the guise of following the supposedly more objective algorithmic recommendations.

Algorithmic governance's lack of transparency, explainability, and legibility contributes to public distrust and impinges upon the consent of the governed, which is the source of legitimacy for public institutions in liberal democratic systems. Danaher has called this the "threat of algocracy," that is, "a situation in which algorithm-based systems structure and constrain the opportunities for human participation in, and comprehension of, public decision-making" (Danaher, 2016, p. 246). Alongside limits to transparency, algorithms' relative inflexibility when compared to jurisprudential principles of interpretation and attention to contextual nuance represent "not only a fundamental incompatibility, but a logical irreconcilability between algorithmic governance and the structure of our legal systems" (Sinnreich, 2018, p. 182). From a law-in-computation perspective, the shift toward algorithmic governance represents a fundamental reorientation of our relationship to data and the law in which "control then works at levels far past the purview of liberal individualism,

situating subjects within networks of power that govern indirectly and without proximity" (Cheney-Lippold, 2011, p. 176).

In the following sections, we discuss algorithmic governance in relation to jurisdiction and agency through a series of case studies.

3 | JURISDICTION: SOVEREIGNTY AND LOCALIZATION

It is easy to imagine that computational systems reside "in the cloud" or in the digital ether that surrounds us. A law-in-computation approach that considers algorithmic governance and its relationship to law, society, and justice can better analyze how actual-world jurisdictions and the people who populate them are represented in data topographies—that is, the data representation of spaces and places from which data are collected and about which governance decisions are made.

In data topographies, people are made visible to institutions through data points and algorithmic processes that interpret the significance of individual behaviors with respect to observed outcomes and within jurisdictional parameters. In this sense, algorithmic outputs "flatten" complex social relationships into collections of data points that come to represent certain types of spaces, and thus are the means by which data topographies are made "field[s] of intervention in which . . . one tries to affect, precisely, a population" (Foucault, 2007, p. 21). For example, municipal governments around the world invest in "smart city" technologies that are part and parcel of digital surveillance and algorithmic governance strategies. Beginning in 2015, New York City replaced a number of public pay phone locations with "LinkNYC" kiosks that offer free Wi-Fi access, free domestic telephone calls, USB charging ports, and interactive digital maps of the city (Brandom, 2015). LinkNYC's kiosks are owned and operated by an Alphabet-subsidiary called Sidewalk Labs, which collects location and behavior data from everyone who uses the kiosks' services and leverages those data for targeted advertising. Thus, LinkNYC is part public infrastructure, part private surveillance; it is a data collection instrument that impacts the relationship between citizens and their actual-world environments. As data scientist Green (2019) argues, "In the emergent smart city, with sensors and cameras on every street corner . . . if you want to avoid being tracked, you must opt out of public space" (p. 99).

Private companies are not the only organizations that can make use of smart city technologies to create data topographies. Criminal justice systems can utilize "factors such as where you spend time, how late you stay out at night, and whether you participated in a particular protest—data that you may never have even known was being collected, and whose collection you certainly never consented to—[to] influence the sentence you are given" (Green, 2019, p. 106). For example, PredPol, a predictive policing algorithm developed by mathematicians, criminologists, and social scientists, uses crime report data to generate "heat maps" on which the algorithm anticipates where crimes are likely to occur. Law enforcement agencies laminate these data-driven renderings of space onto neighborhood maps in order to better optimize resource and officer deployments. As a risk assessment tool that combines big data practices with algorithmic analysis to support decision-making in criminal justice, PredPol is a practical example of the law in computation. Not only are these algorithmic systems integrated into governmental and legal apparatuses that bolster what some activist groups have called "the Stalker State" (Stop LAPD Spying Coalition, 2018; see also Brayne, 2017), but they also shift individuals' expectations about what their presence and behavior in actual-world spaces entails regarding the criminal justice system's capacity to act via computational means. When complemented by digital surveillance technologies such as closed-circuit television cameras and facial recognition software, predictive policing tools afford opportunities for ever-more granular enforcement of rules and regulations within a given jurisdiction with "no commensurate reconsideration

of laws and penalties to counterbalance this escalation" (Sinnreich, 2018, p. 186; see also Graham & Wood, 2003).

Though some LSS attention has been paid to these processes of surveillance, data collection, and decision-making, less has been observed or argued about the politics and/or impact of where law enforcement, government, personal, and corporate data are physically stored, or how these processes have the potential to reconfigure legal definitions of privacy and/or property.

3.1 | Topographies of data processing

Data servers' actual-world locations and their relationships to jurisdiction are anything but arbitrary. Rather, it is imperative to ask where in the world computational systems are located in order to determine which legal frameworks are at play and how this may impact their use and accessibility. In the age of cloud computing, computation is almost always mediated by the internet (Boellstorff, 2010). Sociologist Vincent Mosco (2015, p. 208) warns against giving in to the meteorological imagery of cloud computing, arguing that these images create the sense that the cloud is "a place of no place" and "the home of data stored and processed everywhere and nowhere." Data do not take care of themselves. They are managed by a number of actual-world information and communication infrastructures such as international data centers (Vonderau, 2018) and oceanic fiber optic cables (Starosielski, 2015). These infrastructures and the data that they mediate are governed by policies and laws put in place by both private firms and national governments that critically affect how those data can be used, as well as the rights of the individuals represented by those data.

According to what Vonderau (2018) has called the "topography of data processing"—a mode of geographically mapping how data moves between data centers and end users—the distance and remoteness of cloud infrastructures produces an assumed neutrality of data centers and servers, bolstered by continually reproduced visions of an ethereal, ubiquitous cloud. Yet, Vonderau (2018, p. 705) writes, "this obscures the fact that apart from economic interests inscribed into cloud infrastructure itself, processes of data storage are hardly neutral in regard to data security and privacy, among other issues." Increasingly, national governments are establishing rules and laws for how data must be processed when they flow across borders. Because the cloud enables fragmentation and is made up of complex data flows, it also generates a number of jurisdictional challenges with respect to how geography "matters" in the cloud (Amoore, 2018), where data are located ("data residence"), what country data are in ("data sovereignty" and "data localization"), and to whom the data belongs ("data ownership"), all of which have different implications at personal, institutional, national, and international scales. Strategic movement and placement of data is a mode of governance; many corporations are now multinational in the sense that they either own or utilize data centers located in different places around the world. In setting up this kind of globally distributed infrastructure, they are beholden to different local policies and laws for how data are processed, managed, stored, and backed up.

Public policy and economics scholars have weighed in on a number of legal issues related to cloud computing, including where the infrastructure of the cloud is geographically located and the handling of health data across borders (Seddon & Currie, 2013), data jurisdiction and privacy (Bradshaw et al., 2011; Nelson, 2009; Vaile, 2014), extraterritorial jurisdiction and questions around the governance and security of citizen data across borders (Choo, 2014; Walden, 2013), government surveillance (Jaeger et al., 2008; Jaeger et al., 2009), and the ownership of data in the cloud (Reed, 2010). However, rather than pertaining to the politics or legal ramifications of data topography, most of the issues raised stem from concerns around the misuse of data, a problem prominently debated following Edward Snowden's revelations about the

US National Security Agency's PRISM surveillance program. Governments have responded to these concerns by putting measures in place to control how residents' data are stored and processed, such as the General Data Protection Regulation (GDPR) implemented by the EU in 2018 and the California Consumer Privacy Act of 2018. Centrally storing sensitive personal data on servers that are physically located within national borders has, essentially, created myriad new forms of digital border control.

3.2 | Data sovereignty and localization

We focus here on two formal structures of data governance that are at the forefront of conversations about cloud computing and the law: data sovereignty and data localization. Data sovereignty policies stipulate that information stored in digital form is subject to the laws of the national jurisdiction where it is physically held. This is not so much about the security of data, but rather how they are managed, duplicated, and processed, as well as who maintains control over them or allows them to be moved from one place to another (De Filippi & McCarthy, 2012). There is currently no global standard for data sovereignty, so levels of control are fragmented across different countries, making it difficult to keep up with the varying rules that are in place in an increasingly dispersed cloud.

A recent case provides an illustration of how sovereignty can impede legal access to data and justice across jurisdictions. In 2013, the US government attempted to obtain emails that were believed to contain incriminating evidence of drug trafficking. However, the Microsoft servers that held these data were located in Ireland because the suspect registered their anonymous user account as a resident of Ireland rather than the United States. In July 2016, the US Court of Appeals ruled in favor of Microsoft, deciding the US government had no right to the data because its search warrants had domestic boundaries, and denied government extraterritorial jurisdiction. The US Department of Justice appealed the ruling to the Supreme Court, arguing that according to the Stored Communications Act of 1986—which authorizes law enforcement to access electronic information with a warrant—they had permission to view the emails. Though the Act addresses ways in which internet service providers can store information on devices like servers, it does not account for those devices' actual-world locations. In a blog post regarding the case, Microsoft's President and Chief Legal Officer elaborated on this issue, writing, "The current laws were written for the era of the floppy disk, not the world of the cloud" (Smith, 2017).

Ultimately, the dispute never made it to the Supreme Court, because in 2018, Congress passed the Clarifying Lawful Overseas Use of Data (CLOUD) Act, which requires multinational companies (like Microsoft) to provide law enforcement agencies with any requested data about a US citizen stored by the company, regardless of where those data happen to reside. Still, the issue has not been resolved—the Act also affords companies the right to challenge such requests in court if they believe compliance would violate privacy rights in foreign jurisdictions.

Data localization laws require data about a nation's residents to be collected, processed, and/or stored inside the country before they can be moved or transferred internationally. For companies that own and operate cloud computing services (often with users located in countries all over the world), such laws are seen as burdensome, limiting how personal data can be collected or processed without establishing local data storage facilities. This threatens the integrity of networks that rely on redundancy, wherein data are backed up to servers that may be located in countries other than the country in which the primary server is located. Localization also exposes private data about individual residents to security vulnerabilities, because "centralizing vast quantities of information in a limited number of data centers within a jurisdiction creates an enticing target for those seeking illicit access" (Fraser, 2016, p. 363). Thus, this mode of data

centralization becomes an issue not only of storage and reliability, but also one of access, security, and privacy.

Data sovereignty and localization issues help dismantle the notion that the cloud is without borders and "stateless," bringing to light the actual-world locations of data centers and their relations to geographic borders, jurisdictional issues, and governing legal frameworks. Under localization laws, many countries are starting to specify what classes of data must be processed through local servers, including Russia (all personal data), China (personal, business, and financial data), Australia (health data), Germany (telecommunications metadata), Nigeria (all government data), and Canada (all personal data), among others. These practices tend to Balkanize the internet, fragmenting what is imagined as a global network in the "cloud" into separate, distinct internets. This not only results in delays, inefficiencies, higher costs, and redesigns of internet infrastructure but also brings about new forms of digital border control.

In 2015, for example, the Russian government instituted a new law stipulating that all data relating to its citizens must be stored on servers physically located in Russia. The law is difficult to enforce, and its application is broad, applying to any entity, local or foreign, that stores or processes the personal data of Russian citizens. To comply, foreign companies holding Russian data must establish local data servers within Russian borders, raising concerns about whether and how Russia could break off from the global internet and establish a Russian intranet that is easier for it to control (Fraser, 2016). The consequences of this legal restructuring include its impact on the blogging platform LiveJournal, which was purchased in 2006 by SUP Media, a Russian-owned and Kremlin-associated company. After Russia's new data localization laws went into effect, SUP Media moved the LiveJournal servers to Russia to comply with new data localization regulations, which generated criticism and concern over censorship of the platform's American users by the Russian government. Because LiveJournal is the primary blogging platform for Russian dissidents, the Russian government has intervened in its operations, censoring dissent and LGBTQ-related content (Hoffmann, 2017).

3.3 | Drones, metadata assassinations, and "killer robots"

One of the starkest cases of law in computation where questions about law, technology, and jurisdiction converge is the use of algorithmic warfare, including lethal autonomous weapon systems (LAWS) and drones designed to assess metadata collected in (and out) of war zones. This is an area of national security that in most countries is de facto opaque and inflexible. Because algorithmic warfare is a legal gray area and its use is typically part of top-secret government programs, this area of inquiry typically falls to scholars in conflict studies or political science, outside of the general purview of LSS. Yet, similar programs are now being employed by federal agencies in the United States for immigration enforcement, though (as far as we are aware) they are currently limited to location tracking (Tau & Hackman, 2020). Drones in and of themselves do not constitute a form of algorithmic governance. However, their targeting algorithms, lack of transparency, and association with LAWS (colloquially known as "killer robots") raises a number of critical questions about the ethics and/or legality of data collection by the military within and about other jurisdictions in or out of warzones, how data jurisdiction policies may come to be applied to algorithmic warfare across geopolitical boundaries, the extent of legal accountability for killing suspected terrorists or other "threats" based on algorithm calculations, and the willingness of military personnel to outsource decision-making authority to algorithmic decision-making systems (see Crawford, 2013a, 2013b; Gregory, 2011).

According to leaked NSA PowerPoint slides of the SKYNET program, ML algorithms designed to determine each zones' probability of "terrorist-ness" were utilized in US drone strikes for "targeted killing campaigns" *outside* of declared war zones in Yemen, Pakistan, and Somalia.[4] Under SKYNET, the United States conducted a mass collection of mobile phone

SIM card metadata and used algorithms to determine a suspected person's probability of "terrorist-ness" before deciding whether or not to strike (Scahill, 2015; for analysis, see Grothoff & Porup, 2016). The military employed drones that flew over parts of Pakistan gathering information on 40 million users and stored the information on NSA cloud-based servers. They then ran ML algorithms to identify probable terrorists based on the metadata collected, including travel patterns, "behavior-based analytics" (e.g., having only incoming calls, powering phones down frequently), and "other enrichments," such as having common contacts and going on regular overnight trips. Often, these algorithms served as the *sole* basis for determining whether or not to do a strike, determining the life or death of a suspected target and entailing potential destruction of the space and community around them.

Vladeck predicts that "how the law chooses to treat machines without principles will be the central legal question that accompanies the introduction of truly autonomous machines" (Vladeck, 2014, p. 150). Besides implications for jurisdiction, the use of LAWS, AI, and ML algorithm-enabled drones presents problems tied to agency, rights, and legal personhood by activating algorithmic processes beyond our immediate view and removing human agency from computational decision making. Leveringhaus (2016) describes the distinction between warfare algorithms *executing* and *generating* a targeting decision. The former entails an AI drone deciding between targets already deemed legitimate by a human programmer, applying the laws of war criteria before deployment. Though human judgment is involved, this is still problematic because it assumes that the drone's decision-making algorithm is somehow objective and neutral rather than contextually bound by a programmer's bias—a kind of "god-trick" (Haraway, 1988). *Generating* a targeting decision, on the other hand, differs in that the drone must apply laws of war criteria on its own, assess whether or not a given person is a legitimate target, and then calculate whether a particular course of action is likely to cause excessive harm to those around the target. Either way, when it comes to lethal decision making in warfare, the algorithms used are practically illegible to those who use them—their programming is almost completely opaque to political and military decision makers. These and other algorithms of war suffer from the problems of "dirty data," reproducing existing patterns of discrimination and inheriting the prejudice of how the program is written. Therefore, even in the context of war, transparency about exactly how and why life and death decisions are being made is difficult (if not impossible) to access or decipher. If algorithmic governance involves the willingness to outsource decision-making authority to algorithm-based decision-making systems, LAWS is the ultimate life and death manifestation of this.

To address the extent to which human agency is removed from computational systems, practitioners, programmers, and theorists have attempted to work around dilemmas of removing human judgment, often by mandating that the ultimate arbiter of a decision be a person, not a machine. Citron and Pasquale (2014) outline how military theorists define this human oversight, identifying three categories of weapons: *human-in-the-loop*, which require human commands for targeting and strikes; *human-on-the-loop*, which can make targeting and strike decisions on their own that a human may override; and *human-out-of-the-loop*, which are purely automated and require no human input. However, as became evident with SKYNET, even human-in-the-loop ML algorithms can produce catastrophic results, leading to unnecessary loss of life and little accountability for targeting nonterrorists (see also Brennan-Marquez et al., 2019). Maintaining meaningful human control appears to be essential until such a time when scholars and practitioners can adequately lay the legal groundwork to understand how we as a society tackle dilemmas of robotic agency and the auditability of algorithms, and until it becomes widely understood that algorithms are not abstract rational entities, but are already imbued with prejudiced values and unique social meaning.

4 | AGENCY: ACTUARIAL SUBJECTS, DIGITAL IDENTITIES, AND ALGORITHMIC LABOR

As an alternative to the human-in-the-loop paradigm, Green and Chen call for an "algorithm-in-the-loop" analysis of automated systems that considers how "instead of improving computation by using humans to handle algorithmic blind spots . . . [systems] improve human decisions by using computation to handle cognitive blind spots," prioritizing "the human's decision over the algorithm's as the most important outcome" (Green & Chen, 2019, pp. 97–98).[5] While an algorithm-in-the-loop perspective draws attention to faulty implementation of data-driven governance tools that rely on system-based algorithms, it simultaneously raises questions and opens new areas for LSS inquiry about the agency of automated systems' *objects*—that is, the individuals and groups about whom decisions are made.

A law-in-computation approach that treats law, society, and computational systems in tandem should consider how agency and identity interrelate in complex sociotechnical systems. That is, how agency and identity are determined, what transforms them, and how they are put to use.

4.1 | Actuarial subjects

More than three decades ago, Simon argued that

> Individuals, once understood as moral or rational actors, are increasingly understood as locations in actuarial tables of variations. This shift from moral agent to actuarial subject marks a change in the way power is exercised on individuals by the state and other large organizations. Where power once sought to manipulate the choices of rational actors, it now seeks to predict behavior and situate subjects according to the risk they pose. (Simon, 1988, p. 772)

The concept of the actuarial subject is especially germane to the current era of big data and algorithmic governance with respect to how organizations exercise power through processes of quantification, and in which "the citizen imagined by these organizations is to be shaped, empowered and activated as a participative co-producer of personalized . . . services, whose data from such forms of participation can then be collected and calculated in a constant feedback loop in order to further automate and tailor future services through anticipatory algorithms" (Williamson, 2014, pp. 308–309).

Contemporary actuarial subjects do have a degree of agency with respect to algorithmic classification, including adaptive behaviors like "signaling"—that is, employing certain techniques to make themselves appear more favorably to an algorithm that is evaluating them. To improve their credit score, for example, people can pay their bills on time, keep their credit card balances low, and only request credit reports from reporting agencies authorized to provide them. However, the ability to send these sorts of signals is not equally distributed to everyone because it can be constrained by socioeconomic and other factors. The limits, then, on what is known in ML as actors' capacity for "strategic manipulation" introduce new forms of inequality vis-à-vis algorithmic governance: "Just as an algorithm's use of certain features differentially advantages some populations over others, the room for strategic response that is inherent in many automated systems also naturally favors social groups of privilege" (Hu et al., 2019, p. 259).

Institutions that rely on algorithmic processes for automated decision-making are well aware that they are vulnerable to strategic manipulation, so they invest in ways to counteract that manipulation, typically by making their models' decision boundaries more conservative and making it more difficult for users to achieve a favorable evaluation, further enabling

unequal distribution. Returning to the credit score example, research has shown that Black borrowers in the United States tend to have lower scores than White borrowers even if they repay loans at comparable rates because there is an unequal distribution of outcome likelihoods across racial subpopulations. That is, these models "[raise] the loan threshold to protect against strategic behavior, [thereby increasing] the relative burden on [Blacks]" (Milli et al., 2019, p. 237).

Moreover, if an algorithm makes an unfavorable evaluation—or worse, an inaccurate, incorrect, or injurious one—the difficulty an individual might encounter in fixing the situation represents yet another restriction on human agency. Indeed, there appears to be general consensus among lawmakers that individuals should have the right to challenge algorithmic decisions. Article 79 of the European Union's GDPR, for example, states that "each data subject shall have the right to an effective judicial remedy where he or she considers that his or her rights . . . have been infringed as a result of the processing of his or her personal data."[6] However, the onus for identifying rights infringements and bringing such challenges tends to lie with the individual, not with the decision maker.[7] Moreover, the ability to challenge algorithmic decisions does not necessarily mean that there are *actionable* means for recourse. If, for example, the desired outcome can only be obtained by changing an algorithmic variable like age or racial identity, then recourse cannot reasonably be considered actionable because these are typically immutable characteristics. The degree to which an automated decision-making model makes recourse possible, then, is a significant measure of the relative agency that individuals have under algorithmic governance.

The concept of the actuarial subject prefigures the implications that algorithmic governance tools have for identity, particularly how they construe token-type relationships between individuals and populations. This digital sorting and categorization "results in the creation of subjects through databases that do not replicate or imitate the original subject but create a multiplicity of selves that may be acted upon without the knowledge of the original" (Graham & Wood, 2003, p. 230). Cheney-Lippold has called this "a new algorithmic identity," that is, "an identity formation that works through mathematical algorithms to infer categories of identity on otherwise anonymous beings . . . [such that] it moves the practice of identification into an entirely digital, and thus measurable, plane" (Cheney-Lippold, 2011, p. 165).

The capacity for ML algorithms and automated decision makers to "[induce] a rule from an entire population's behavior that can then be applied to specific individuals" (Barocas et al., 2013, p. 6) makes "calculated publics" possible, in which "the algorithmic presentation of publics back to themselves shape[s] a public's sense of itself" (Gillespie, 2014, p. 168). In other words, algorithmic classification can engender a performative orientation in those whom it classifies. Online visibility and the accessibility of digital mugshots, for instance, affects not only how arrestees are viewed in society at large but also how they see themselves, leading some to avoid familial and community responsibilities because of the stigma associated with their arrest photos (Lageson, 2016). Predictive algorithms and risk assessment tools, such as those used in the criminal justice system (Hannah-Moffat, 2018; Lum & Isaac, 2016; Selbst, 2017) and in financial services (Citron & Pasquale, 2014; Fuster et al., 2017), contribute to one's digital identity insofar as they calculate scores that assign individuals certain statuses within a larger population (e.g., low risk for recidivism, high risk of defaulting on a loan, etc.).

Algorithms do not simply produce identities in *comparison* to others; they also draw upon an individual's relationships *with* others to make these determinations (Boyd et al., 2014). As discussed above, SKYNET's use of drones to surveil populations suspected of terrorism predicted terrorist activity based on metadata partially based on their degree of contact with *one another*. Other predictive algorithms interpret data from social media profiles to assess an individual's credit risk as a function of their broader social networks. This "creditworthiness by association" analysis (Hurley & Adebayo, 2016, p. 151) introduces new possibilities for discrimination, as the algorithm translates data points about others as constitutive of an individual's

identity. In these cases, individuals have even less agency in regard to information about their family and friends than they do over their own behaviors and status.[8]

4.2 | Biometrics technology and the proliferation of digital legal IDs

In the wake of 9/11 and the subsequent "war on terror," there was an exponential increase in the deployment of biometric technologies, or "automated systems that use biological or behavioral characteristics to identify individuals," particularly for securitizing borders (Wilson, 2006, p. 87). Biometrics are designed to digitally capture, store, and then authenticate physiological, chemical, and behavioral features—often called "imprints"—unique to individuals, including faces, iris and retina patterns, DNA, gait,[9] fingerprints, and voice patterns, among others. They are used to both verify (i.e., confirm that someone is who they say they are), and to identify (i.e., determine who a person is), "invest[ing] the biological body with the assumed capacity to truthfully speak for itself and reveal its identity proper" (Pugliese, 2010, as cited in Pötzsch, 2015, p. 105). As physical borders' dependence on marked territories and walls decreases, "iBorder" regimes of inclusion and exclusion depend on biometrics to mark and sort out good and bad mobility, wanted and unwanted people, and deserving and undeserving immigrants (Pötzsch, 2015; also see Zureik & Salter, 2005).

Though the proliferation of biometric technologies is especially evident at international borders, they now reach across entire national populations: iPhone users log in to their phones using Face ID, municipalities are integrating facial-recognition software with security cameras on city streets and in sports arenas, and several countries now require "smart" national identity cards embedded with personal identifiers. These types of biometric technology do not just aggregate or store identifiers but use algorithms to transform imprints and audiovisual files into a "template" that is stored in the system's server where it can be compared to others. As previously stated, there is evidence to suggest that these technologies do not always do this accurately. Acquisition parameters for algorithmic biometric technology primarily use able-bodied white men as template subjects (Pugliese, 2010); at least three commercial facial recognition programs were recently shown to demonstrate high margins of error when faced with dark-skinned women (Buolamwini & Gebru, 2019). Besides its own use of ML algorithms, biometric technology is used in conjunction with other algorithmic tools such as arrest records, health data, and databases used for predictive policing. These developments raise questions about how the use of biometrics will continue to shape sociolegal landscapes surrounding privacy, citizenship, social control, and, in the case of growing digital ID systems, access to benefits, citizenship rights, and legal personhood.

One of the most ambitious and controversial national digital identity projects to date is India's Aadhaar program, which assigns to every Indian citizen a unique 12-digit identifier that is reinforced by biometric and demographic data.[10] On the one hand, advocates argue that Aadhaar provides a measure of security against identity theft and that it helps to streamline the business of government while preventing corruption. On the other hand, although it was initially introduced as a voluntary program in 2009, the Indian government has made a number of decisions over the past decade—such as linking Aadhaar cards to direct benefit transfers—that necessitate having an Aadhaar number in order to receive public services. The Aadhaar Act of 2016 granted the program legal status, making enrollment all but mandatory.

In 2017, building on programs like Aadhaar and other regional initiatives such as ID4Africa,[11] the Rockefeller Foundation, Accenture, and Microsoft entered a public-private partnership with agencies of the UN, governments, and nongovernmental organizations (NGOs) to develop the "ID2020 campaign," aimed at broadening and democratizing what they call the *right* to a digital identity (see Accenture, 2017; Roberts, 2017). According to organizers, the development of an international digital identity regime promises "legal identity for all" in

fulfillment of UN Sustainable Development Goal Target 16.9 (ID2020, 2018). Since its launch, the World Bank has also initiated its own very similar campaign called ID4D (Identification for Development).[12] Each initiative claims that developing a global database of personal data and biometrics from populations around the world (e.g., headshots, fingerprints, and retina scans) will help secure citizen identification systems, improve international development, and protect vulnerable populations such as refugees, trafficking victims, and stateless and displaced populations who do not have access to paperwork or identity documentation.

Along these lines, ID2020 aims to develop an international infrastructure of so-called *digital legal identities* on a shared, digitized ledger made accessible to multiple governments and global institutions responsible for managing citizenship, economic development, and migration (e.g., UNHCR, the World Bank) within and across borders. To ensure that digital identities cannot be hacked or altered, ID2020 partners such as Microsoft promise that these digital IDs will be safely secured using blockchain technology (Roberts, 2017). Blockchain, as originally devised by the creators of the digital currency Bitcoin, provides an open, decentralized database in which data's authenticity is verified by the entire network of its users rather than a third party, keeping data integrity in check because all users are informed if/when the master ledgers do not match. In other words, blockchain will (in theory) distribute global digital identities across borders without worry that states, corrupt officials, or other hackers can steal them or make unauthorized changes (see Miller, 2017).

The argument goes that digitizing IDs via ID2020 will, much like Aadhaar, help citizens access critical services such as education and health care, circumventing situations in which people lack access to their national IDs or birth certificates; have their documents denied, lost, destroyed, or stolen; and/or (in the case of displaced persons) have no way of proving who they are. UN agencies such as the UN High Commissioner for Refugees (UNHCR) began digitizing the records of displaced persons about a decade ago, supplementing refugee registration records and fingerprint data with biometrics such as headshots and retina scans (see Lodinova, 2016). Refugee registration, according to UNHCR, ensures that proper records are kept of displaced peoples' status; can protect refugees from forced return, arbitrary arrest, or detention; and provides access to refugee services such as food and medical assistance. In 2018, the agency reported that their biometric database, called PRIMES, had 6.5 million registered individuals, with 54 countries participating (UNHCR, 2018). Access to these existing databases, however, is limited to the UN agencies that use them. ID2020 proposes that biometric data and digital legal identities should be internationally accessible—to states, officials, and citizens—because they are superior to paper-based records. That is, they are persistent and portable across borders, and due to biometrics they are (according to proponents) secure without needing to rely on a single state or government entity to vouch for an individual's identity on paper documents.

Two issues concerning digital ID infrastructures like ID2020 that are ripe for LSS analysis include their implications for increased cross-border state surveillance and control, and questions about whether an international infrastructure created by international governmental organizations (IGOs), NGOs, and corporations can/will succeed in protecting citizenship or formal identity without the participation of states, which would turn traditional notions of state sovereignty, citizenship, and legal personhood on their head.

First, though proponents argue that initiatives such as ID2020, ID4D, and Aadhaar will benefit citizens and vulnerable populations, they also point to ways in which digital identities will ensure *citizen* compliance, benefiting states and governmental institutions. For example, Aadhaar is often pitched as a means of ensuring that "persons [can]not create 'duplicates' of themselves to claim more than their share of state subsidies or other goods" (L. Cohen, 2017, p. 301). Critics, however, argue that Aadhaar's technocratic solution to governance actually infringes upon privacy and exposes personal data to risks and vulnerabilities, especially as the government has made the Aadhaar database available to third parties (Satpathy, 2017). Similarly, although ID2020 focuses the core of its public-facing campaign on the provision of basic

human rights (i.e., the right to an identity) for displaced populations, its objectives undoubtedly raise questions about the proposed infrastructure's implications for new and renewed forms of domestic and cross-border state surveillance. Similar to debates about predictive policing, surveillance, and cyber law enforcement, here lies a tension between the emancipatory potential of new technologies and debates about technology being used to surveil, control, and distinguish between "desirable" and "undesirable" populations (Dumbrava, 2017; Hu, 2017). Rather than emancipate vulnerable populations, history suggests that digital ID infrastructures are likely to reproduce existing inequalities, "serv[ing] as technological signifiers of the securitization of migration" (Wilson, 2006, p. 98).

There are situations in which migrants, political refugees, or asylum seekers fleeing persecution may not *want* to be found, tracked, or identified by corrupt or rights-violating state officials. Unlike a password or pin that safeguards financial data or private documents, it is nearly impossible to correct biometric data if it is hacked, manipulated or ultimately "misread" by algorithmic software. By situating digital identities in such a way as to mitigate false identities and deny (or punish, or deport) those who "cheat" the aid system, ID2020 undermines the claim that digital identities are meant to ensure rights, instead "mobilizing [biometric technologies] within a larger 'tough on crime' style rhetoric that posits [migrants] as fraudulent and criminal" (Wilson, 2006, p. 99). In other words, because the public-facing campaign focuses attention on displaced populations, the implication is that all people, but *especially* migrants, must be sorted, tracked, authenticated, and analyzed for the purpose of risk profiling.

Second, the claim that the establishment of digital legal IDs distributed by blockchain technology will, in and of itself, "create" and evenly distribute legal identities for all overlooks the realities of statelessness and the value of legal personhood and citizenship in today's global political economy. Similar to treating cloud computing as if data servers did not require a physical space or jurisdiction, the claims made by ID2020 seemingly assume that by establishing digital biometric data files and storing them in the "digital ether" of the cloud (seemingly "outside" of national borders) will (on its own) grant legal identity, regardless of whether a given person has been granted legal personhood and/or citizenship by a given state authority. While it may be true that digital identities have the potential to benefit those who do not have access to *existing* national identity documents, this does not work if a person was never granted a legal identity to begin with.

Indeed, there are approximately 12 million stateless individuals who have no legal identity at all—that is, they are not considered nationals or citizens of any state (UNHCR, 2003). Some are migrants and refugees; many are not. Stateless people do not lack identity because their paperwork is "lost" but because they were not granted a legal identity under the law in the first place, often due to corruption, conflicts between legal regimes, the politics of international surrogacy (see Dumbrava, 2017), and/or discriminatory practices related to place of birth, gender, race, or ethnicity. Under ID2020, it is probable that stateless people will either remain invisible, or alternatively, that they will simply be captured in the database as "stateless persons"—a categorization that, in the existing political economy, means little and excludes the individual from state citizenship and legal personhood. Although UNHCR and other UN agencies have long recognized the problem of statelessness and have sought to provide benefits to these groups, receiving a "stateless" designation does not necessarily require that any state or welfare institution actually grant them any social benefits, civil rights, or citizenship. Indeed, legal identity and citizenship remain out of reach for most stateless people and refugees throughout their lifetimes, functioning as "an intergenerational carrier of civic and social exclusion" (Costello, 2017, p. 718). Therefore, suggesting that capturing biometric data and distributing it over a secured, shared ledger will somehow override the global politics of inclusion, exclusion, and citizenship obscures and ignores power; alternatively, it proposes that we will soon live in a world where legal personhood and citizenship are no longer granted by the state but by an external source of international authority

Digital identity regimes—and, for that matter, big data collected via social media, digital payment systems, and mobile telephony—can be algorithmically processed and used to automate decisions that impact an individual's opportunities. This highlights the importance of being able to control which data are collected under which conditions, how data are used, and how long data are stored as a measure of agency in the age of big data. Incorporating a law-in-computation approach to more LSS scholarship can help make sense of emergent reactions and adaptations to digital identity regimes and the like, demonstrating where and when these tools fail to fulfill their promise and how they are integrated into the contemporary exercise of state power.

4.3 | Virtual work and algorithmic labor management

In addition to digital IDs, the emergence of digital labor marketplaces and the increasing share of the global labor force engaged in virtual work have transformed workers' identities and agency, both affectively and legally. While the term "virtual work" can refer to most of the remote jobs that gained prominence in the 1990s and 2000s—such as call center work and software outsourcing—a new wave of virtual work enabled by websites and smartphone applications has allowed thousands of people to look for and provide services through intermediary digital platforms such as Uber, Taskrabbit, Amazon Mechanical Turk, and others. These platform-based labor arrangements represent a growing share of the so-called "gig economy," characterized by flexible, contingent, and typically short-term contracts, lack of employer-provided benefits (e.g., health insurance, childcare, or retirement savings), and inconsistent compensation rates. Whereas legal scholars have primarily asked how regulatory frameworks in the gig economy should apply to protocols and online behavior, J. Cohen (2017) argues that these are the wrong questions: "Core legal institutions *are already evolving* in response to [the] ongoing transformations [offered by platform economies]," so questions should not be about how the law should apply to gig economies, but how they are already transforming law at the institutional level (p. 136). "Law for the platform economy is already being written—not via discrete, purposive changes, but rather via the ordinary, uncoordinated but self-interested efforts of [workers, lawyers, and lobbyists]" (J. Cohen, 2017, p. 136).

Platform companies do not claim to be in the business of employment or workforce management. Rather, they claim to be digital aggregators, merely providing a marketplace for potential customers and vendors to find each other (see De Stefano, 2015). In the United States, these vendors are legally defined as independent contractors who enter voluntarily into employment arrangements with individuals or organizations that purchase their labor temporarily. As such, they are not considered employees of the platform operator and so do not enjoy any guarantees or protections extended to workers under statutes like the Fair Labor Standards Act or the National Labor Relations Act (Felstiner, 2011). As gig work expands, the global economy moves toward a future of nonstandard, precarious employment where risk is increasingly privatized, transferred onto individuals, and kept outside of employee–employer contracts.

The terms used to describe these forms of atypical employment differ across national contexts and extant labor codes and frameworks, and they often entail dramatically different legal statuses for workers. In the United Kingdom, casual employment contracts are popularly known as "zero-hour contracts," a term also used in Australia, New Zealand, and Canada (Brinkley, 2013). In the United States, gig workers are sometimes called "1099 workers" because they report income on 1099-MISC forms in their tax filings, whereas wage and salaried employees typically report earnings on W-2 statements. These ambiguities regarding gig workers' statuses and the obligations that platforms have to them in different jurisdictions have provoked a number of legal challenges. For example, in response to a class action lawsuit brought forth by Uber drivers, judges at the UK's Court of Appeal ruled that Uber drivers

should be considered workers rather than independent contractors and should be entitled to sick pay, holiday pay, and parental leave (Varghese, 2018). Similar lawsuits have been mounted against rideshare platforms in the United States, alleging that on-demand platform companies have misclassified their workers as independent contractors in order to extract more value from them without guaranteeing job security (Reiff, 2018). California's Assembly Bill 5, which the state legislature passed in 2019, establishes a legal framework for classifying some categories of gig work like ridesharing based primarily on the degree of agency that workers have with respect to the platforms that they use. The bill has been opposed by platform companies such as Uber and Lyft, and at the time of this writing it is unclear how the law will be enforced and whether companies will comply with it fully.

Outside of the technical challenge of (mis)classifying workers, there is a larger argument about whether older classification categories fully capture the exigencies and motivations of workers who come to platform work seeking more flexibility, questions that dovetail with LSS research on labor law and workers' rights in creative industries (Fisk, 2003), temporary employment (Gonos, 1997), and split labor markets (Auerhahn, 1999). Being bound by employee contracts would make different demands on workers' time and presence, something that platform companies claim would be detrimental to workers.[13] Depending on the motivations and constraints that each worker faces with respect to their productivity, the push for employee classification could impact workers as much as it affects' platform companies' profit margins. Against this backdrop, there have been proposals to create a third or "hybrid" labor category in the United States somewhere between employee and independent contractor that responds to the demands created by contemporary socioeconomic and technological realities (Aloisi & Cherry, 2016; Dubal, 2017).

The platform technologies that virtual gig workers rely upon have also ushered in their own set of challenges regarding how traditional employee–employer relationships are managed.[14] In particular, many virtual work platforms make use of ML algorithms to "perform a variety of supervisory tasks from the mundane to the sophisticated: assigning tasks to workers, speeding up work processes, determining the timing and length of breaks, monitoring quality, ranking employees, and much more" (Cherry & Poster, 2016, pp. 294–295). Algorithmic labor management techniques like these are designed to maximize worker productivity by measuring speed and diligence, automating task assignment based on those metrics (De Stefano, 2018). Several of these platforms also integrate rating and reputation systems to exercise a degree of control over workers who use their technologies to find gigs, even though there is little evidence to suggest that ratings have significant informational value (Adams-Prassl, 2019). Customers are encouraged to rate the quality of the services they received, and those ratings are then used to afford the worker more gig opportunities or, alternatively, to limit their options. A recent study of platform workers in the Global South found that "workers with the best scores and the most experience tended to receive more work due to clients' preferences and the platforms' algorithmic ranking of workers within search results" (Wood et al., 2018, p. 64). In this way, gig workers' agency is constrained not only by arrangements with their nominal "employer"—in this case, a virtual work platform—but also by the whims of those who purchase their services through the platform via forms of algorithmic labor management.[15]

Algorithmic governance of labor and workplaces depends on digital surveillance and monitoring of workers. For example, as Levy (2015) explores in her work on the US trucking industry, as AI-powered systems are introduced to maximize efficiency within logistics and delivery, truckers "are increasingly subjected to performance monitoring via fleet management systems that record and transmit fine-grained data about their location and behaviors" (p. 160). In hospitals, municipal public works departments, and elsewhere, workers are required to wear GPS-enabled devices that track their locations in real time (Ajunwa, 2018), and in some cases these devices record health data that companies use to suggest wellness regimes to their employees (Ajunwa et al., 2017). These tools and the data that they generate belong to an emerging area

of interest that some scholars have labeled "people analytics," that is, "an approach to human resources management using huge pools of quantitative data, rather than simply managerial judgment or personal assessment" (Bodie et al., 2017, p. 964). The integration of people analytics into workplaces not only has obvious implications for personal privacy but also provides an early glimpse into what the biopolitical management of bodies and labor may look like when workers are no longer accountable to a single or limited set of entities (e.g., a human boss, customers) but are instead continually monitored by automated decision-making systems that are themselves made, serviced, and sold by third parties to logistics companies.

Like digital legal IDs, the shift toward virtual work, platform labor, and the algorithmic management tools and techniques that enable them raise a host of legal questions—and challenges—concerning, among other things, individual rights, privacy, autonomy, and how these new forms of work are transforming the law from the bottom up. Attending to these questions will be critical to a law-in-computation approach to LSS.

5 | DISCUSSION AND CONCLUSION

In 1910, Roscoe Pound published "Law in Books and Law in Action," (Pound, 1910) a powerful salvo into the debates over the seeming capriciousness of court rulings on the constitutionality of statutes. Pound inaugurated a kind of social jurisprudence that demanded consideration of the social effects of legal practice. In Pound's day, labor rights were a hotly contested issue. "Law in Books and Law in Action" specifically references the *Lochner* case (Lochner v. New York, 198 U.S. 45), which invalidated a New York State law limiting the working hours of bakers in favor of the right to freedom of contract. In the 1960s, the phrase "law on the books and law in action" reentered sociological jurisprudence with the rise of the Law and Society Movement (see Abel, 2010; Garth & Sterling, 1998; Trubek, 1990), in which social science attempted to grapple with law and legal process in the context of the War on Poverty and the civil rights movement. If we can argue that the shift from "law on the books" to "law in action" was precipitated by concerns about labor rights and civil rights, then the shift we are calling for in this article is precipitated by a growing concern over algorithmic rights: that is, how to assess claims and remedies in the context of an algorithmic saturation of law and society.

The era of algorithmic governance is not a distant prospect cooked up by science fiction writers. It has already arrived, and in all likelihood it will continue to grow in intensity and scope for the foreseeable future. The previous generation of LSS scholars inaugurated a paradigm shift by bringing social scientific analysis to the law. We have proposed a new paradigm shift, turning LSS attention to technological developments through the study of "law in computation." As big data–driven AI, ML, and automated decision-making systems continue to develop and be implemented in data management, warfare, citizenship, and labor contexts, these technologies will become ever more indispensable to the practice of law.

As the presented cases demonstrate, the study of algorithmic governance tools and systems is broad. Data sovereignty and data localization laws provide private and public institutions with opportunities for "data arbitrage," which involves exploiting different jurisdictional affordances in actual-world locations in order to extract value from data and avoid restrictions on their use. LAWS systems recast notions of agency and accountability in warfare and challenge questions of international law. Digital identity regimes present new forms of population management dressed up in liberal democratic human rights discourse, while the visibilities that these regimes afford have the potential to harm as well as help. And algorithmic controls that complement the growing arena of virtual work introduce new modes of biopolitical management of labor. We have highlighted two problem areas—jurisdiction and legal agency—but by no means should these be taken to be exhaustive of approaches to the law in computation. These only serve as a handful of examples, demonstrating the myriad ways in which the law in computation is not simply a matter of academic curiosity but is also of great civic importance.

Alongside specific integrations, law in computation must attend to the new statutes, regulations, and judicial decisions concerning algorithmic governance. It is a well-worn cliché that the speed of innovation moves more quickly than the speed of legislation, and so the law is continually playing "catch-up" with new technologies. Kroll et al. (2017) argue that "the tools currently available to policymakers, legislators, and courts were developed primarily to oversee human decision makers," and thus are inadequate to the task of holding automated decision-making systems accountable (p. 636). A number of current and pending regulations seek to address algorithmic governance's legal implications, and these will no doubt shape the direction of law in computation research in the near future. As discussed above, the European Union's GDPR and California's Consumer Privacy Act are arguably the most comprehensive pieces of legislation to date that outline individuals' rights with respect to data that are generated and collected about them by both public and private organizations. Although both of these laws are technically only applicable within specific jurisdictions—the European Union and the state of California, respectively—any entity that does business within those jurisdictions is also subject to them. Given that large technology and media companies (e.g., Google, Facebook, Amazon, etc.) operate virtually anywhere with an internet connection, both the GDPR and California's consumer protection laws have impacts far beyond their borders.

Still, neither the GDPR nor the Consumer Privacy Act is sufficient on its own to resolve all of the problems regarding fairness, accountability, and transparency that emerge with the shift toward algorithmic governance. While it is possible to analyze data inputs and system outcomes, there are no regulatory mechanisms for auditing how algorithms *process* data, and therefore no public oversight that could potentially identify problems in real time (Caplan et al., 2018). The Algorithmic Accountability Act of 2019 (H.R. 2231), introduced in the US House of Representatives in April 2019, is one example of an attempt to require any organization that uses automated decision making to perform regular assessments of both their data protection procedures and potential biased or discriminatory impacts of their systems. Observers have lauded the act's ambitions while noting its shortcomings regarding details about consultations with external auditors and compliance with assessment results (Selbst et al., 2019). At the time of this writing, however, the act has yet to be referred to a committee and looks unlikely to be passed any time soon.

Moreover, some of the potential technological solutions for bias and inequality in algorithmic governance would actually violate current antidiscrimination statutes, particularly the provisions in Title VII of the US Civil Rights Act of 1964 that outlaw disparate treatment and impact with respect to certain sensitive attributes (e.g., race, gender, sex, religion, etc.). The legal standard for fairness that Title VII establishes is crucial for ensuring that organizations cannot discriminate, whether intentionally or unintentionally, but it also fails to account for structural inequalities that affect individual opportunity. And while these restrictions provide an important check on automated decision-making systems by prohibiting the design and integration of intentionally discriminatory tools, they can also, counterintuitively, impede optimization for certain fairness constraints. Researchers have demonstrated through experimentation that allowing an ML model to consider legally defined sensitive attributes of protected classes can actually, in some cases, increase predictive accuracy while avoiding bias (Dwork et al., 2018). As Hoffman (2019, p. 901) has argued, "In mirroring some of antidiscrimination discourse's most problematic tendencies, efforts to achieve fairness and combat algorithmic discrimination fail to address the very hierarchical logic that produces advantaged and disadvantaged subjects in the first place." However, so long as antidiscrimination law remains in its current form, eliminating bias in the design of algorithmic governance tools must be achieved on the front end of the design process "because users of algorithms may be legally barred from revising processes to correct for discrimination after the fact" (Kroll et al., 2017, p. 692). Given large corporations' recent stance against using systems known for algorithmic biases—as evidenced by the actions of IBM, Amazon, and Microsoft following protests against racial

TABLE 2 Future research topics and methods

Area of inquiry	Future research topics	Possible LSS frameworks	Methods
Algorithmic governance	Smart cities, facial recognition and surveillance, automated decision making in the public sector	Legal realism, legal/judicial decision-making, critical race/feminist perspectives	FOIA requests, collaborative research with activist groups and legal aid societies, surveys or qualitative interviews with civilians/users/experts
Jurisdiction	Data arbitrage, legality and/or accountability for algorithmic warfare	Legal pluralism, legal geography, legal compliance, law and security, international law	Comparison of national or local laws governing AI/ML/algorithms, institutional or organizational analysis
Agency	Implementation of digital identity regimes, algorithmic labor management; symbolic compliance with regulations against algorithmic bias	Access to justice, biopolitics, governmentality, social control, endogeneity, and symbolic structures of compliance	Participant observation, ethnographic interviews, algorithmic auditing, adversarial design/ counterfactual experimentation

Abbreviations: AI, artificial intelligence; FOIA, Freedom of Information Act; ML, machine learning.

profiling and the death of George Floyd (see Greene, 2020)—one possible direction for future LSS research in this area may be to analyze the process by which organizations publicly respond to critiques of algorithmic discrimination as they simultaneously mediate ways to comply with laws designed to regulate racial bias (see Edelman, 1992).

Pursuing a law-in-computation approach to analyzing these and other emergent issues presents an opportunity for interdisciplinary research and advocacy that can anticipate the non-immediate and diverse encounters that big data and algorithmic governance systems may produce (see Table 2). Such a reorientation would not only be useful for progressive and long-lasting jurisprudence but would also make currently available jurisprudence "transformative" by reckoning with the fundamental effects of computational logics and techniques (Solow-Niederman et al., 2019). Emerging algorithmic governance phenomena, such as the proliferation of smart city technologies, facial recognition surveillance, increased personalization of services based on big data analytics, and the digitalization of legal and political processes, are all topics that are currently marginal or siloed to separate disciplines. However, they demand a more comprehensive law-in-computation approach that brings together disciplinary expertise from computer and data science, legal studies, and the social sciences. Though we have primarily described the dangers and limitations of the law in computation, technology can theoretically—if empowered to do so—also be used to keep those in power accountable.

An interdisciplinary LSS focus on the law in computation has the benefit of drawing from the strengths of its contributing disciplines, which include, but are not limited to, sociology, anthropology, international relations, history, law, and, we propose, science and technology studies. Contributions may include bringing topics into analyses of the law in computation that are traditionally siloed to individual disciplines. For example, as discussed previously, the study of warfare has traditionally belonged to political science, but the use of algorithmic decision-making by drones may serve as a useful case for criminologists and sociolegal scholars interested in analyzing their use by immigration enforcement agencies. Qualitative information science scholars and anthropologists of technology such as Burrell (2016), Seaver (2019), and Dourish (2016), among others, have championed democratic approaches to studying algorithmic systems that do not hinge upon revealing the truth of blackboxed systems. Approaches such as "algorithms in culture" as well as "AI on the Ground"[16] treat algorithmic systems as social,

economic, and political "matters of concern" while accounting for their uncertain epistemic and ontological status. Sociologist Juan Pablo Pardo-Guerra (2012), who has studied the automation of modern stock markets, has also drawn attention to the moral, political, and organizational struggles that actively shape how computation systems "make landfall" (Starosielski, 2015).

Tried and true research methods, from comparative legal analysis to participant observation, will remain useful, but the tools of algorithmic governance demand—and afford— new methodologies that adapt, borrow or and/or extend the strengths and limitations of LSS's contributing disciplines. Large-scale projects that analyze algorithmic processes while drawing on big data can undoubtedly learn from the nuances provided by participant observation, interviewing, and ethnographic methods in anthropology and sociology, which could be useful for analyzing virtual worlds, evaluating end-user effects, and the otherwise contributing to the work of data scientists, designers, and programmers (see Boellstorff et al., 2012; Passi & Sengers, 2020; Sloane & Moss, 2019). Similarly, qualitative scholars drawing from ethnographic data would benefit from a better understanding of how algorithmic processes work on a large scale, as well as the analytic and methodological possibilities offered by big data. Law and society scholars interested in the social processes involved in developing algorithms could perhaps audit algorithms in partnership with computer and/or data scientists.[17]

Methodological interventions could also include LSS scholars submitting FOIA requests to review algorithms used by public institutions—as Legal Aid of Arkansas did when preparing its case against the state's Medicaid reform—collaborating with local activist groups and legal aid societies, organizing participatory, adversarial design projects through "hackathons" (DiSalvo, 2012; Lodato & DiSalvo, 2016), or experimenting with counterfactuals (Wachter et al., 2018). Researchers achieved an important legal victory in March 2020 when the US District Court for the District of Columbia ruled in Sandvig v. Barr that auditing algorithms to uncover discrimination against protected classes does not violate the Computer Fraud and Abuse Act, opening the door for more independent review of AI and ML in order to find evidence of disparate impacts and hold institutions accountable (American Civil Liberties Union [ACLU], 2020).

A thorough sociotechnical engagement with the law in computation is also crucial to realizing radical decolonial politics while examining and critiquing these technologies. LSS scholars cannot merely be token figures at the table but need to tactically engage with information infrastructures and the role of nonhuman agency in a serious manner (Raval, 2019). In many instances, legal responses to platform effects have been reactionary at best, seeking out a human entity (the company CEO, the local manager, etc.) or the corporation as such and placing the onus of responsibility and blame on a human or a group of humans (see also Elish, 2019). In their recent Congressional testimonies, Facebook's Mark Zuckerberg and Google's Sundar Pichai spent most of their time explaining how technology works and then attributing liability to unexpected platform effects, including the subversion of "community standards" set by each company by malicious individuals and groups (Youn, 2019).

Innovations in AI and big data also produce challenges for the continuing struggles of Indigenous communities and their representatives, who have been calling for the recognition of Indigenous data sovereignty, especially given how computing technologies shift and morph property relations with regard to personal and nonpersonal data (Kukutai & Taylor, 2016; Walter & Suina, 2019). These writings need not remain footnotes to the canonical approaches to law and technology; as we go forward, such crises in LSS can provide generative spaces in which to foreground the longstanding concerns and demands made by indigenous communities as well as disabled persons and others with regard to datafication.

As shown here, algorithmic governance, technological innovations, and automated decision-making present a number of technological and legal concerns for contemporary societies. The continually shifting intersections between computational processes and creative human

agency have implications for how concepts such as jurisdiction, privacy, and property, among others, are defined and accounted for under the law. Just as the law cannot keep pace with the speed of technological developments, new technologies also compete with, and are the products of, human ingenuity, making this a dynamic research space. Given that big data, AI, and ML are here to stay, the work of LSS scholars informed by a law-in-computation approach can act as a critical check against the potential for these technologies to do harm rather than work in the public interest.

ACKNOWLEDGMENTS

The authors would like to express their sincere gratitude to Bill Maurer and Mona Lynch for their ongoing feedback and support on this project. We would also like to thank Christopher J. Bates; participants of the 2018 Technology, Law and Society Summer Institute at the University of California, Irvine for brainstorming and collaborating with us on the project; and our anonymous reviewers for their careful reading and feedback. This material is based upon work supported by the National Science Foundation under grant no. SES-1724735. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Science Foundation.

ORCID

Tania DoCarmo https://orcid.org/0000-0002-9128-7646
Stephen Rea https://orcid.org/0000-0002-2732-6014
Noopur Raval https://orcid.org/0000-0002-7934-5559

ENDNOTES

[1] Use cases for fully automated adjudication—let alone regulation—are limited at the moment, though there is potential for them to be expanded in the near future. See Coglianese and Lehr (2019) for a more detailed discussion.

[2] As public scrutiny of Clearview AI intensified, investigative journalists uncovered evidence of CEO Cam-Hoan Ton-That's ties to far-right extremists, further complicating the company's agenda and its integration with law enforcement via a contract with Immigration and Customs Enforcement (O'Brien, 2020).

[3] The use of "actual-world" throughout the article follows the distinction that Boellstorff draws between concepts of "virtual" and "actual" with respect to digital culture, and in which the "actual world" "refer[s] to places of human culture not realized by computer programs through the Internet" (Boellstorff, 2008, p. 21).

[4] Access to the PowerPoint slides of the SKYNET program can be found at *The Intercept*, "SKYNET: Courier Detection via Machine Learning" and "SKYNET: Applying Advanced Cloud-based Behavior Analytics" at https://theintercept.com/document/2015/05/08/skynet-courier/ and https://theintercept.com/document/2015/05/08/skynet-applying-advanced-cloud-based-behavior-analytics/.

[5] Rahwan pushes for a "society-in-the-loop" approach that is focused on "embedding the values of society, as a whole, in the algorithmic governance of societal outcomes that have broad implications," such as allocating economic resources and labor, managing autonomous transportation technologies, or filtering news and information (Rahwan, 2018, p. 7).

[6] Article 82 of the GDPR further stipulates that "[a]ny person who has suffered material or non-material damage . . . shall have the right to receive compensation from the controller or processor for the damage suffered."

[7] Wachter et al. (2017) argue that the GDPR lacks a strict mandate that automated decision-making systems be explicable, only requiring that individuals receive "meaningful information about the significance, envisaged consequences, and logic involved" in a decision, but not case-by-case explanations (p. 83). This could limit individuals' abilities to hold systems accountable if they do not have the technical expertise to parse automated decisions. Others disagree, however, and contend that the GDPR does in fact include a right to explanation (Selbst & Powles, 2017; see also Doshi-Velez et al., 2017).

[8] There is an assumption made in associational analysis that social network correlations are valuable signals rather than statistical noise. As Boyd and Crawford observe, however, these analyses may amount to little more than "seeing patterns where none actually exist, simply because massive quantities of data can offer connections that radiate in all directions" (Boyd & Crawford, 2011, p. 2).

[9] See Voth (2003).

[10] See "Unique Identification Authority of India." *Government of India*. https://uidai.gov.in/.

[11] See "Identity for All in Africa." *ID4Africa*. https://id4africa.com/.

[12] See "ID for Development." *World Bank*. https://id4d.worldbank.org/.

[13] In her research on US-based Uber and Lyft drivers, Rosenblat (2018) has noted a range of motivations and levels of commitment among rideshare drivers, who range from full-time drivers to part-time drivers to hobbyist workers.

[14] For criticism of platform work and an alternative vision of platform cooperatives, see Schneider and Scholz (2016).

[15] Some activists have developed digital tools that invert rating and reputation systems' power dynamics to a certain extent, empowering platform workers to rate clients—see Silberman et al. (2010) for an example of how this practice has been deployed for Amazon Mechanical Turk workers.

[16] See "AI on the Ground." *Data & Society*. https://datasociety.net/research/ai-on-the-ground/.

[17] Sandvig et al. (2014, p. 18) propose five methods for auditing algorithms that depend on different levels of access to source code. However, they also note that the current regulatory environment makes it difficult to audit proprietary algorithms, and so they call for creating "a kind of algorithm observatory acting for the public interest" that would have a mandate to do this kind of oversight (Sadvig et al., 2014, p. 18).

REFERENCES

Abel, Richard L. **2010**. "Law and Society: Project and Practice." *Annual Review of Law and Social Science 6* (1): 1–23.

Accenture. **2017**. "Accenture, Microsoft Create Blockchain Solution to Support ID2020: Companies Team on Digital Identity Program." https://newsroom.accenture.com/news/accenture-microsoft-create-blockchain-solution-to-support-id2020.htm.

Adams-Prassl, Jeremia. **2019**. "What If Your Boss Was an Algorithm? Economic Incentives, Legal Challenges, and the Rise of Artificial Intelligence at Work." *Comparative Labor Law & Policy Journal 41* (1): 1–30.

Ajunwa, Ifeoma. **2018**. "Algorithms at Work: Productivity Monitoring Applications and Wearable Technology as the New Data-Centric Research Agenda for Employment and Labor Law." *Saint Louis University Law Journal 63*: 21–54.

Ajunwa, Ifeoma, Kate Crawford, and Jason Schultz. **2017**. "Limitless Worker Surveillance." *California Law Review 105*: 735–76.

Aloisi, Antonio, and Miriam A. Cherry. **2016**. "A Third Employment Category for On-Demand Workers?" Oxford Business Law Blog. https://www.law.ox.ac.uk/business-law-blog/blog/2016/11/third-employment-category-demand-workers.

American Civil Liberties Union (ACLU). **2020**. "*Federal Court Rules 'Big Data' Discrimination Studies Do Not Violate Federal Anti-hacking Law*." New York: ACLU. https://www.aclu.org/press-releases/federal-court-rules-big-data-discrimination-studies-do-not-violate-federal-anti.

Amoore, Louise. **2018**. "Cloud Geographies: Computing, Data, Sovereignty." *Progress in Human Geography 42* (1): 4–24.

Aronson, Jay D. **2018**. "Computer Vision and Machine Learning for Human Rights Video Analysis: Case Studies, Possibilities, Concerns, and Limitations." *Law & Social Inquiry 43* (4): 1188–209.

Auerhahn, Kathleen. **1999**. "The Split Labor Market and the Origins of Antidrug Legislation in the United States." *Law & Social Inquiry 24* (2): 411–40.

Bailenson Jeremy N., Blascovich Jim, Beall Andrew C., Noveck Beth. **2006**. Courtroom Applications of Virtual Environments, Immersive Virtual Environments, and Collaborative Virtual Environments. *Law & Policy 28* (2): 249–270. http://dx.doi.org/10.1111/j.1467-9930.2006.00226.x.

Barocas, Solon, Sophie Hood, and Malte Ziewitz. **2013**. "Governing Algorithms: A Provocation Piece." *SSRN*: 2245322. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2245322.

Barocas, Solon, and Andrew D. Selbst. **2016**. "Big Data's Disparate Impact." *California Law Review 104*: 671–732.

Bhalerao, Rasika, Maxwell Aliapoulios, Ilia Shumailov, Sadia Afroz, and Damon McCoy. **2019**. "Mapping the Underground: Supervised Discovery of Cybercrime Supply Chains." Paper presented at the annual Anti-phishing Working Group Symposium on Electronic Crime Research (eCrime), Pittsburgh, PA, November 13–15.

Biddle, Sam. **2020**. "ICE's New York Office Uses a Rigged Algorithm to Keep Virtually All Arrestees in Detention." *The Intercept*, March 2, 2020. https://theintercept.com/2020/03/02/ice-algorithm-bias-detention-aclu-lawsuit/.

Bodie, Matthew T., Miriam A. Cherry, Marcia L. McCormick, and Jintong Tang. **2017**. "The Law and Policy of People Analytics." *University of Colorado Law Review 88*: 961–1042.

Boellstorff, Tom. **2008**. *Coming of Age in Second Life: An Anthropologist Explores the Virtually Human*. Princeton, NJ: Princeton University Press.

Boellstorff, Tom. **2010**. "Culture of the Cloud." *Journal for Virtual Worlds Research 2* (5): 4–9.

Boellstorff, Tom, Nardi, Bonnie, Pearce, Celia, and Taylor, Tina L. **2012**. *Ethnography and virtual worlds: A handbook of method*, Princeton: Princeton University Press.

Boyd, Danah, and Kate Crawford. **2011**. "Six Provocations for Big Data." *A Decade in Internet Time: Symposium on the Dynamics of the Internet and Society*: Oxford Internet Institute. https://dx.doi.org/10.2139/ssrn.1926431

Boyd, Danah, Karen Levy, and Alice Marwick. **2014**. "The Networked Nature of Algorithmic Discrimination." In *Data and Discrimination: Collected Essays*, edited by Seeta Peña Gangadharan, Virginia Eubanks, and Solon Barocas, 53–7. Washington, DC: Open Technology Institute/New America.

Bradshaw, Simon, Christopher Millard, and Ian Walden. **2011**. "Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services." *International Journal of Law and Information Technology 19* (3): 187–223.

Brandom, Russell. **2015**. "New York Is Finally Installing Its Promised Public Gigabit Wi-Fi." *The Verge*. December 28, 2015. https://www.theverge.com/2015/12/28/10674634/linknyc-new-york-public-wifi-installation-photos-gigabit.

Brayne, Sarah. **2017**. "Big Data Surveillance: The Case of Policing." *American Sociological Review 82* (5): 977–1008.

Brayne, Sarah, Karen Levy, and Bryce Clayton Newell. **2018**. "Visual Data and the Law." *Law & Social Inquiry 43* (4): 1149–63.

Brennan-Marquez, Kiel, Karen Levy, and Daniel Susser. **2019**. "Strange Loops: Apparent Versus Actual Human Involvement in Automated Decision-Making." *Berkeley Technology Law Journal 34*: 745–72.

Brinkley, Ian. **2013**. *Flexibility or Insecurity? Exploring the Rise in Zero Hours Contracts*. Lancaster, UK: The Work Foundation.

Buolamwini, Joy, and Gebru, Timnit. **2018**. Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. *Proceedings of the 1st Conference on Fairness, Accountability and Transparency, PMLR 81* 77–91. http://proceedings.mlr.press/v81/buolamwini18a.html.

Buolamwini, Joy, and Timnit Gebru. **2018**. "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification." *Proceedings of Machine Learning Research 81*: 1–15.

Burrell, Jenna. **2016**. "How the Machine 'Thinks': Understanding Opacity in Machine Learning Algorithms." *Big Data & Society 3* (1): 1–12.

Cameron, Dell. **2020**. "Vermont Seeks Injunction against Clearview AI, Says Firm Broke Multiple State Laws." *Gizmodo*, March 11, 2020. https://gizmodo.com/vermont-seeks-injunction-against-clearview-ai-says-fir-1842274874.

Caplan, Robyn, Joan Donovan, Lauren Hanson, and Jeanna Matthews. **2018**. *Algorithmic Accountability: A Primer*. New York, NY: Data & Society.

Cheney-Lippold, John. **2011**. "A New Algorithmic Identity: Soft Biopolitics and the Modulation of Control." *Theory, Culture & Society 28* (6): 164–81.

Cherry, Miriam A., and Winifred R. Poster. **2016**. "Crowdwork, Corporate Social Responsibility, and Fair Labor Practices." In *Research Handbook on Digital Transformations*, edited by F. Xavier Olleros and Majilinda Zhegu, 291–312. Northampton, MA: Edward Elgar Publishing.

Choo, Kim-Kwang Raymond. **2014**. "A Cloud Security Risk-Management Strategy." *IEEE Cloud Computing 1* (2): 52–6.

Citron, Danielle Keats, and Frank Pasquale. **2014**. "The Scored Society: Due Process for Automated Predictions." *Washington Law Review 89*: 1–33.

Coglianese, Cary, and David Lehr. **2019**. "Transparency and Algorithmic Governance." *Administrative Law Review 71*: 1–56.

Cohen, Julie. **2017**. "Law for the Platform Economy." *UC Davis Law Review 51*: 133–204.

Cohen, Lawrence. **2017**. "Duplicate." *South Asia: Journal of South Asian Studies 40* (2): 301–4.

Coldicutt, Rachel. **2018**. "Why Data Legibility Is More Important than Explainability." *Doteveryone,* October, 15, 2018. https://medium.com/doteveryone/data-legibility-and-a-common-language-coping-not-coding-part-2-8afb687de60.

Costello, Cathryn. **2017**. "On Refugeehood and Citizenship." In *The Oxford Handbook of Citizenship*, edited by Ayelet Shachar, Rainer Bauböck, Irene Bloemraad, and Maarten Vink. Oxford: Oxford University Press.

Crawford, Neta. **2013a**. *Accountability for Killing: Moral Responsibility for Collateral Damage in America's Post-9/11 Wars*. New York: Oxford University Press.

Crawford, Neta. **2013b**. *Damage in America's Post-9/11 Wars*. Oxford, UK: Oxford University Press.

Danaher, John. **2016**. "The Threat of Algocracy: Reality, Resistance and Accommodation." *Philosophy & Technology 29* (3): 245–68.

Danaher, John, Michael J. Hogan, Chris Noone, Rónán Kennedy, Anthony Behan, Aisling De Paor, Heike Felzmann, et al. **2017**. "Algorithmic Governance: Developing a Research Agenda through the Power of Collective Intelligence." *Big Data & Society 4* (2): 1–21.

De Filippi, Primavera, and Smari McCarthy. **2012**. "Cloud Computing: Centralization and Data Sovereignty." *European Journal of Law and Technology 3* (2): 1–18.

De Stefano, Valerio. **2015**. "The Rise of the 'Just-in-Time Workforce': On-Demand Work, Crowdwork, and Labor Protection in the 'Gig-Economy.'" *Comparative Labor Law & Policy Journal 37*: 471–503.

De Stefano, Valerio. **2018**. "'Negotiating the Algorithm': Automation, Artificial Intelligence, and Labor Protection." *International Labour Office*, EMPLOYMENT Working Paper No. 246.

Desai, Deven R., and Joshua A. Kroll. **2017**. "Trust but Verify: A Guide to Algorithms and the Law." *Harvard Journal of Law & Technology 31* (1): 1–64.

DiSalvo, Carl. **2012**. *Adversarial Design*. Cambridge, MA: The MIT Press.

Doshi-Velez, Finale, Mason Kortz, Ryan Budish, Chris Bavitz, Sam Gershman, David O'Brien, Stuart Shieber, James Waldo, David Weinberger, and Alexandra Wood. **2017**. "Accountability of AI Under the Law: The Role of Explanation." In *Berkman Klein Center Working Group on Explanation and the Law*. Berkman Klein Center for Internet & Society Working Paper. https://dash.harvard.edu/handle/1/34372584

Dourish, Paul. **2016**. "Algorithms and Their Others: Algorithmic Culture in Context." *Big Data & Society 3* (2): 1–11.

Dubal, Veena B. **2017**. "Winning the Battle, Losing the War?: Assessing the Impact of Misclassification Litigation on Workers in the Gig Economy." *Wisconsin Law Review 2017*: 740–802.

Dumbrava, Costica. **2017**. "Citizenship and Technology." In *The Oxford Handbook of Citizenship*, edited by Ayelet Shachar, Rainer Bauböck, Irene Bloemraad, and Maarten Vink. Oxford, UK: Oxford University Press.

Dunn, Meghan A., Peter Salovey, and Neal Feigenson. **2006**. "The Jury Persuaded (and Not): Computer Animation in the Courtroom." *Law & Policy 28*: 228–48.

Dwork, Cynthia, Nicole Immorlica, Adam Tauman Kalai, and Max Leiserson. **2018**. "Decoupled Classifiers for Group-Fair and Efficient Machine Learning." Paper presented at the Conference on Fairness, Accountability, and Transparency, New York, NY, February 23–24.

Edelman, Lauren B. **1992**. "Legal Ambiguity and Symbolic Structures: Organizational Mediation of Civil Rights Law." *American Journal of Sociology 97* (6): 1531–76.

Elish, Madeleine Clare. **2019**. "Moral Crumple Zones: Cautionary Tales in Human–Robot Interaction." *Engaging Science, Technology, and Society 5*: 40–60.

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

Felstiner, Andrew. **2011**. "Working the Crowd: Employment and Labor Law in the Crowdsourcing Industry." *Berkeley Journal of Employment & Labor Law 32* (1): 143–204.

Fisk, Catherine L. **2003**. "Authors at Work: The Origins of the Work-for-Hire Doctrine." *Yale Journal of Law & the Humanities 15*: 1–70.

Foucault, Michel. **2007**. *Security, Territory, Population: Lectures at the Collège de France 1977–1978*. New York, NY: Picador.

Fraser, Erica. **2016**. "Data Localisation and the Balkanisation of the Internet." *SCRIPTed 13*: 360–73.

Fuster, Andreas, Paul Goldsmith-Pinkham, Tarun Ramadorai, and Angsar Walther. **2017**. "Predictably Unequal? The Effects of Machine Learning on Credit Markets." CEPR Discussion Paper No. DP12448 London: Centre for Economic Policy Research. https://cepr.org/active/publications/discussion_papers/dp.php?dpno=12448

Garth, Bryant, and Joyce Sterling. **1998**. "From Legal Realism to Law and Society: Reshaping Law for the Last Stages of the Social Activist State." *Law & Society Review 32* (2): 409–72.

Gillespie, Tarleton. **2014**. "The Relevance of Algorithms." In *Media Technologies: Essays on Communication, Materiality, and Society*, edited by Tarleton Gillespie, Pablo J. Boczkowski, and Kristen A. Foot, 167–93. Cambridge, MA: The MIT Press.

Gonos, George. **1997**. "The Contest of Employer Status in the Postwar United States: The Case of Temporary Help Firms." *Law & Society Review 31* (1): 81–110.

Graham, Stephen, and David Wood. **2003**. "Digitizing Surveillance: Categorization, Space, Inequality." *Critical Social Policy 23* (2): 227–48.

Green, Ben. **2019**. *The Smart Enough City: Putting Technology in Its Place to Reclaim Our Urban Future*. Cambridge, MA: The MIT Press.

Green, Ben, and Yiling Chen. **2019**. "Disparate Interaction: An Algorithm-in-the-Loop Analysis of Fairness in Risk Assessments." Annual Conference on Fairness, Accountability, and Transparency (FAT*), Atlanta, GA, January 29–31.

Greene, Jay. **2020**. "Microsoft Won't Sell Police Its Facial-Recognition Technology, Following Similar Moves by Amazon and IBM." *The Washington Post*, June 11, 2020. Accessed July 6, 2020. https://www.washingtonpost.com/technology/2020/06/11/microsoft-facial-recognition/.

Gregory, Derek. **2011**. "From a View to a Kill: Drones and Late Modern War." *Theory, Culture & Society 28* (7–8): 188–215.

Grothoff, Christian, and J. M. Porup. **2016**. "The NSA's SKYNET Program May Be Killing Thousands of Innocent People." *Ars Technica*, February 16, 2016. https://arstechnica.com/information-technology/2016/02/the-nsas-skynet-program-may-be-killing-thousands-of-innocent-people/.

Hannah-Moffat, Kelly. **2018**. "Algorithmic Risk Governance: Big Data Analytics, Race and Information Activism in Criminal Justice Debates." *Theoretical Criminology 23* (4): 453–70.

Haraway, Donna. **1988**. "Situated Knowledges: The Science Question in Feminism and the Privilege of Partial Perspective." *Feminist Studies 14* (3): 575–99.

Hassan, Samer, and Primavera De Filippi. **2017**. "The Expansion of Algorithmic Governance: From Code Is Law to Law Is Code." *Field Actions Science Reports, Special Issue 17*: 88–90.

Hoffman, Anna Lauren. **2019**. "Where Fairness Fails: Data, Algorithms, and the Limits of Antidiscrimination Discourse." *Information, Communication & Society 22* (7): 900–15.

Hoffmann, Jay. **2017**. "Whatever Happened to LiveJournal?" *The History of the Web*. https://thehistoryoftheweb.com/postscript/whatever-happened-livejournal/.

Hu, Margaret. **2017**. "Algorithmic Jim Crow." *Fordham Law Review 86*: 633–96.

Hurley, Mikella, and Julius Adebayo. **2016**. "Credit Scoring in the Era of Big Data." *Yale Journal of Law and Technology 18*: 148–216.

Hu, Lily, Immorlica, Nicole, and Vaughan, Jennifer Wortman. **2019**. The Disparate Effects of Strategic Manipulation. *Proceedings of the Conference on Fairness, Accountability, and Transparency (FAT* '19)*. 259–268. New York: Association for Computing Machinery. https://dl.acm.org/doi/10.1145/3287560.3287597.

ID2020. **2018**. *ID2020 Alliance: Committed to Improving Lives Through Digital Identity*. Accessed February 7, 2018. https://id2020.org/.

Jaeger, Paul T., Jimmy Lin, and Justin M. Grimes. **2008**. "Cloud Computing and Information Policy: Computing in a Policy Cloud?" *Journal of Information Technology & Politics 5* (3): 269–83.

Jaeger, Paul T., Jimmy Lin, Justin M. Grimes, and Shannon N. Simmons. **2009**. "Where Is the Cloud? Geography, Economics, Environment, and Jurisdiction in Cloud Computing." *First Monday 14* (5). https://journals.uic.edu/ojs/index.php/fm/article/view/2456.

Katz, Daniel Martin. **2013**. "Quantitative Legal Prediction—or—How I Learned to Stop Worrying and Start Preparing for the Data-Driven Future of the Legal Services Industry." *Emory Law Journal 62*: 909–66.

Kluttz, Daniel N., and Mulligan, Deirdre K. **2019**. Procurement as Policy: Administrative Process for Machine Learning. *Berkeley Technology Law Journal 34* (3): 853–890. https://lawcat.berkeley.edu/record/1137218.

Kroll, Joshua A., Joanna Huey, Solon Barocas, Edward W. Felten, Joel R. Reidenberg, David G. Robinson, and Harlan Yu. **2017**. "Accountable Algorithms." *University of Pennsylvania Law Review 165*: 633–705.

Kukutai, Tahu, and John Taylor. **2016**. *Indigenous Data Sovereignty: Toward an Agenda*. Canberra, Australia: Australian National University Press.

Lageson, Sarah E. **2016**. "Found Out and Opting Out: The Consequences of Online Criminal Records for Families." *The ANNALS of the American Academy of Political and Social Science 665* (1): 127–41.

Lecher, Colin. **2018**. "What Happens When an Algorithm Cuts Your Health Care." *The Verge*, March 21, 2018. https://www.theverge.com/2018/3/21/17144260/healthcare-medicaid-algorithm-arkansas-cerebral-palsy.

Lessig, Lawrence. **2006**. *Code: And Other Laws of Cyberspace, Version 2.0*. New York, NY: Basic Books.

Leveringhaus, Alex. **2016**. "Drones, Automated Targeting, and Moral Responsibility." In *Drones and Responsibility: Legal, Philosophical and Socio-Technical Perspectives on Remotely Controlled Weapons*, edited by Ezio Di Nucci and Filippo Santoni de Sio, 169–81. New York, NY: Routledge.

Levy, Karen E. **2015**. "The Contexts of Control: Information, Power, and Truck-Driving Work." *The Information Society 31* (2): 160–74.

Lodato, Thomas James, and Carl DiSalvo. **2016**. "Issue-Oriented Hackathons as Material Participation." *New Media & Society 18* (4): 539–57.

Lodinova, Anna. **2016**. "Application of Biometrics as a Means of Refugee Registration: Focusing on UNHCR's Strategy." *Development, Environment and Foresight 2* (2): 91–100.

Lum, Kristian, and William Isaac. **2016**. "To Predict and Serve?" *Significance 13* (5): 14–9.

Marx, Gary T. **1995**. "The Engineering of Social Control: The Search for the Silver Bullet." In *Crime & Inequality*, edited by J. Hagan and R. Peterson. Palo Alto, CA: Stanford University Press.

McGinnis, John O., and Russell G. Pearce. **2014**. "The Great Disruption: How Machine Intelligence Will Transform the Role of Lawyers in the Delivery of Legal Services." *Fordham Law Review 82*: 3041–66.

Miller, Ron. **2017**. "The Promise of Managing Identity on Blockchain." *TechCrunch*, September 10, 2017. http://social.techcrunch.com/2017/09/10/the-promise-of-managing-identity-on-the-blockchain/.

Milli, Smitha, Miller, John, Dragan, Anca D., and Hardt, Moritz. **2019**. The Social Cost of Strategic Classification. *Proceedings of the Conference on Fairness, Accountability, and Transparency (FAT* '19)*, New York: Association for Computing Machinery. https://dl.acm.org/doi/10.1145/3287560.3287576.

Mosco, Vincent. **2015**. *To the Cloud: Big Data in a Turbulent World*. New York, NY: Routledge.

Nelson, Michael R. **2009**. "The Cloud, the Crowd, and Public Policy." *Issues in Science and Technology 25* (4): 71–6.

O'Brien, Luke. **2020**. "The Far-Right Helped Create the World's Most Powerful Facial Recognition Technology." *HuffPost*, April 7, 2020. https://www.huffpost.com/entry/clearview-ai-facial-recognition-alt-right_n_5e7d028bc5b6cb08a92a5c48.

Pardo-Guerra, Juan Pablo. **2012**. "Financial Automation, Past, Present, and Future." In *The Oxford Handbook of the Sociology of Finance*, edited by Karin Knorr Cetina and Alex Preda. Oxford, UK: Oxford University Press.

Pasquale, Frank. **2015**. *The Black Box Society: The Secret Algorithms That Control Money and Information*. Cambridge, MA: Harvard University Press.

Passi, Samir, and Phoebe Sengers. **2020**. "Making Data Science Systems Work." *Big Data & Society 7* (2): 1–13.
Pötzsch, Holger. **2015**. "The Emergence of iBorder: Bordering Bodies, Networks, and Machines." *Environment & Planning D: Society & Space 33* (1): 101–18.
Pound, Roscoe. **1910**. "Law in the Books and Law in Action." *American Law Review 44*: 12–36.
Pugliese, Joseph. **2010**. *Biometrics: Bodies, Technologies, Biopolitics*. London: Routledge.
Rahwan, Iyad. **2018**. "Society-in-the-Loop: Programming the Algorithmic Social Contract." *Ethics and Information Technology 20* (1): 5–14.
Raval, Noopur. **2019**. "An Agenda for Decolonizing Data Science." *Spheres: Journal for Digital Cultures 5*: 1–6.
Reed, Chris. **2010**. "Information 'Ownership' in the Cloud." *Queen Mary School of Law Legal Studies Research Paper*, No. 45. London: QMUL School of Law.
Reiff, Nathan. **2018**. "Recent Lawsuits Could Pioneer Gig Economy Reform." *Wake Forest University School of Law Journal of Business & Intellectual Property Law*, November 5, 2018. http://ipjournal.law.wfu.edu/2018/11/recent-lawsuits-could-pioneer-gig-economy-reform/.
Remus, Dana, and Frank Levy. **2017**. "Can Robots Be Lawyers? Computers, Lawyers, and the Practice of Law." *Georgetown Journal of Legal Ethics 30*: 501–58.
Richardson, Rashida, Jason M. Schultz, and Kate Crawford. **2019**. "Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice." *New York University Law Review Online 94*: 15–55.
Roberts, Jeff John. **2017**. "Microsoft and Accenture Unveil Global ID System for Refugees." *Fortune*, June 19, 2017. https://fortune.com/2017/06/19/id2020-blockchain-microsoft/.
Rosenblat, Alex. **2018**. *Uberland: How Algorithms Are Rewriting the Rules of Work*. Berkeley, CA: University of California Press.
Sandvig, Christian, Kevin Hamilton, Karrie Karahalio, and Cedric Langbort. **2014**. "Auditing Algorithms: Research Methods for Detecting Discrimination on Internet Platforms." Paper presented at the 64th Annual Meeting of the International Communication Association. A preconference on "Data and Discrimination: Converting Critical Concerns into Productive Inquiry," May 22, Seattle, WA.
Satpathy, Tathagata. **2017**. "The Aadhaar: 'Evil' Embodied as Law." *Health and Technology 7* (4): 469–87.
Scahill, Jeremy. **2015**. "The Assassination Complex." *The Intercept*, October 15, 2015. https://theintercept.com/drone-papers/the-assassination-complex/.
Schneider, Nathan, and Trebor Scholz, eds. **2016**. *Ours to Hack and to Own: The Rise of Platform Cooperativism, a New Vision for the Future of Work and a Fairer Internet*. New York, NY: OR Books.
Seaver, Nick. **2019**. "Knowing Algorithms." In *Digital STS: A Field Guide*, edited by Janet Vertesi and David Ribes, 412–222. Princeton, NJ: Princeton University Press.
Seddon, Jonathan J. M., and Wendy L. Currie. **2013**. "Cloud Computing and Trans-border Health Data: Unpacking US and EU Healthcare Regulation and Compliance." *Health Policy and Technology 2* (4): 229–41.
Selbst, Andrew D. **2017**. "Disparate Impact in Big Data Policing." *Georgia Law Review 52*: 109–95.
Selbst, Andrew D., Madeleine Clare Elish, and Mark Latonero. **2019**. "Accountable Algorithmic Futures." *Data & Society Points*, April 19, 2019. https://points.datasociety.net/building-empirical-research-into-the-future-of-algorithmic-accountability-act-d230183bb826.
Selbst, Andrew D., and Julia Powles. **2017**. "Meaningful Information and the Right to Explanation." *International Data Privacy Law 7* (4): 233–42.
Semmler, Sean, and Zeeve Rose. **2017**. "Artificial Intelligence: Application Today and Implications Tomorrow." *Duke Law & Technology Review 16*: 85–99.
Silberman, M. Six, Lilly Irani, and Joel Ross. **2010**. "Ethics and Tactics of Professional Crowdwork." *XRDS 17* (2): 39–43.
Simon, Jonathan. **1988**. "The Ideological Effects of Actuarial Practices." *Law & Society Review 22* (4): 771–800.
Sinnreich, Aram. **2018**. "Four Crises in Algorithmic Governance." *Annual Review of Law and Ethics 26*: 181–90.
Sloane, Mona, and Emanuel Moss. **2019**. "AI's Social Sciences Deficit." *Nature Machine Intelligence 1* (8): 330–1.
Smith, Brad. **2017**. "US Supreme Court Will Hear Petition to Review Microsoft Search Warrant Case while Momentum to Modernize the Law Continues in Congress." Microsoft, October 16, 2017. https://blogs.microsoft.com/on-the-issues/2017/10/16/us-supreme-court-will-hear-petition-to-review-microsoft-search-warrant-case-while-momentum-to-modernize-the-law-continues-in-congress/.
Solow-Niederman, Alicia, YooJung Choi, and Guy Van den Broeck. **2019**. "The Institutional Life of Algorithmic Risk Assessment." *Berkeley Technology Law Journal 34*: 705–44.
Starosielski, Nicole. **2015**. *The Undersea Network*. Durham: Duke University Press.
Starr, Sonja B. **2014**. "Evidence-Based Sentencing and the Scientific Rationalization of Discrimination." *Stanford Law Review 66* (4): 842–72.
Stop LAPD Spying Coalition. **2018**. *Before the Bullet Hits the Body: Dismantling Predictive Policing in Los Angeles*. Los Angeles, CA: Stop LAPD Spying Coalition. Accessed May 8, 2018. https://stoplapdspying.org/wp-content/uploads/2018/05/Before-the-Bullet-Hits-the-Body-May-8-2018.pdf
Surden, Harry. **2014**. "Machine Learning and Law." *Washington Law Review 89*: 87–115.

Tau, Byron, and Michelle Hackman. **2020**. "Federal Agencies Use Cellphone Location Data for Immigration Enforcement." *The Wall Street Journal*, February 7, 2020. https://www.wsj.com/articles/federal-agencies-use-cellphone-location-data-for-immigration-enforcement-11581078600.
Trubek, David M. **1990**. "Back to the Future: The Short, Happy Life of the Law and Society Movement." *Florida State University Law Review 18*: 1–55.
UNHCR. **2003**. *The 1954 Convention relating to the Status of Stateless Persons: Implementation within the European Union Member States and Recommendations for Harmonisation*. Geneva: UN High Commissioner for Refugees (UNHCR).
UNHCR **2018**. "PRIMES Biometric Identity Management: Bi-monthly Update Covering BIMS, IrisGuard, and the Global Distribution Tool." July and August Summary. https://reporting.unhcr.org/sites/default/files/UNHCR%20Biometrics%20Update%20-%20%20July%20August%202018%20.pdf.
Vaile, David. **2014**. "The Cloud and Data Sovereignty after Snowden." *Australian Journal of Telecommunications and the Digital Economy 2* (1): 1–58.
Varghese, Sanjana. **2018**. "Judges Rule Against Uber in Landmark Gig Economy Lawsuit." *WIRED*, December 19, 2018. https://www.wired.co.uk/article/uber-verdict-court-of-appeal-gig-economy.
Vladeck, David C. **2014**. "Machines without Principles: Liability Rules and Artificial Intelligence." *Washington Law Review 89* (1): 117–50.
Vonderau, Asta. **2018**. "Scaling the Cloud: Making State and Infrastructure in Sweden." *Ethnos 84* (4): 698–718.
Voth, Danna. **2003**. "You Can Tell Me by the Way I Walk." *IEEE Intelligent Systems 18* (1): 4–5.
Wachter, Sandra, Brent Mittelstadt, and Luciano Floridi. **2017**. "Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation." *International Data Privacy Law 7* (2): 76–99.
Wachter, Sandra, Brent Mittelstadt, and Chris Russell. **2018**. "Counterfactual Explanations without Opening the Black Box: Automated Decisions and the GDPR." *Harvard Journal of Law & Technology 31* (2): 841–87.
Walden, Ian. **2013**. "Accessing Data in the Cloud: The Long Arm of the Law Enforcement Agent." In *Privacy and Security for Cloud Computing*, edited by Siani Pearson and George Yee, 45–71. London: Springer.
Walter, Maggie, and Michele Suina. **2019**. "Indigenous Data, Indigenous Methodologies and Indigenous Data Sovereignty." *International Journal of Social Research Methodology 22* (3): 233–43.
Williamson, Ben. **2014**. "Knowing Public Services: Cross-Sector Intermediaries and Algorithmic Governance in Public Sector Reform." *Public Policy and Administration 29* (4): 292–312.
Wilson, Dean. **2006**. "Biometrics, Borders and the Ideal Suspect." In *Borders, Mobility and Technologies of Control*, edited by Sharon Pickering and Leanne Weber, 87–109. Dordrecht: Springer.
Wood, Alex J., Mark Graham, Vili Lehdonvirta, and Isis Hjorth. **2018**. "Good Gig, Bad Gig: Autonomy and Algorithmic Control in the Global Gig Economy." *Work, Employment and Society 33* (1): 56–75.
Youn, Bruno G. **2019**. "Catching Congress Up: Restoring the Office of Technology Assessment." B.A. Thesis, Claremont McKenna University.
Zureik, Elia, and Mark B. Salter, eds. **2005**. *Global Surveillance and Policing: Borders, Security, and Identity*. Cullompton, Devon, UK: Willan Publishing.

LAWS CITED

Algorithmic Accountability Act of 2019, H.R. 2231, 116th Cong.
California Assembly Bill 5, A.B. 5, 2019-2020 Leg. Sess., Reg. Sess. (Ca. 2019)
California Consumer Privacy Act of 2018, A.B. 375, 2017-2018 Leg. Less., Reg. Less. (Ca. 2018).
Civil Rights Act of 1964, Pub. L. 88-352, 78 Stat. 241.
Clarifying Lawful Overseas Use of Data Act of 2018, H.R. 4943, 115th Cong.
Freedom of Information Act, 5 U.S.C. § 552 (1966).
General Data Protection Regulation (EU) 2016/679, OJ L 119, 4.5.2016 (2016).
Lochner v. New York, 198 U.S. 45 (1908).
Stored Communications Act, 18 U.S.C.A §§ 2701–2711 (1986).

AUTHOR BIOGRAPHIES

Tania E. DoCarmo is a postdoctoral teaching and research fellow in the Legal Studies Program at the University of Massachusetts Amherst with a PhD in Sociology from University of California Irvine. She studies the intersection of international law, society, and culture, with a focus on migration, citizenship, and human trafficking.

Stephen C. Rea is a researcher and adjunct instructor at the Colorado School of Mines. His research concerns digital culture, focusing on issues in labor and consumer finance from cross-cultural perspectives.

Evan P. Conaway is a PhD candidate in the Department of Anthropology at the University of California, Irvine. His current research centers on the preservation of online video games and other digital media, especially with regard to memory, copyright, museums, and data topography.

John R. Emery is a postdoctoral researcher at Stanford University's Center for International Security and Cooperation (CISAC). His previous work focused on emerging military technology and international law, with current research examining sociotechnical interactions and their impact on moral decision making.

Noopur Raval a postdoctoral researcher at the AINow Institute at New York University. Her research investigates the histories and material contexts of the global AI economy. She has an interdisciplinary background in Media Studies, Information Studies, and Humanities.

How to cite this article: DoCarmo T, Rea S, Conaway E, Emery J, Raval N. The law in computation: What machine learning, artificial intelligence, and big data mean for law and society scholarship. *Law & Policy*. 2021;1–30. https://doi.org/10.1111/lapo.12164