

Algorithmic Governance and the International Politics of Big Tech


Swati Srivastava

Big technology companies like Facebook, Google, and Amazon amass global power through classification algorithms. These algorithms use unsupervised and semi-supervised machine learning on massive databases to detect objects, such as faces, and to process texts, such as speech, to model predictions for commercial and political purposes. Such governance by algorithms—or “algorithmic governance”—has received critical scrutiny from a vast interdisciplinary scholarship that points to algorithmic harms related to mass surveillance, information pollution, behavioral herding, bias, and discrimination. Big Tech’s algorithmic governance implicates core IR research in two ways: (1) it creates new private authorities as corporations control critical bottlenecks of knowledge, connection, and desire; and (2) it mediates the scope of state–corporate relations as states become dependent on Big Tech, Big Tech circumvents state overreach, and states curtail Big Tech. As such, IR scholars should become more involved in the global research on algorithmic governance.

Algorithms are computational rules that allow pilots to fly planes, epidemiologists to monitor disease outbreaks, and web filters to catch spam. Classification algorithms, the focus of this article, use unsupervised and semi-supervised machine learning on massive databases to detect objects, such as faces, and process texts, such as speech, to model predictions. These predictions automate decision-making for commercial purposes, including content visibility and advertising, and for political interests, such as deportations and counterterrorism. In “algorithmic governance,” deference to automated decision-making makes algorithms “a source and factor of social order” (Just and Latzer 2017, 246). A vast interdisciplinary literature has emerged to study the consequences of algorithmic governance for social control (Amoore 2020; Andrejevic 2020; Benjamin 2019; Bucher 2018; Citron and Pasquale 2014; Crawford 2021; Crawford and Schultz 2019; Danaher et al. 2017; Noble 2018; Pasquale 2015; Yeung 2018; Zuboff 2019). International

relations scholarship has identified artificial intelligence (AI; Dafoe 2018), internet governance (DeNardis 2014), privacy regulation (Farrell and Newman 2019; Wong 2020), and technology platforms (Atal 2020; Gorwa 2019) as important research areas. This article argues that IR should pay even more attention to governance by algorithms.

In particular, IR researchers should join scholars from other fields in analyzing the role of the world’s wealthiest corporations—Google, Amazon, Facebook, and Apple (“Big Tech”)—in algorithmic governance, as done by comparativists (Culpepper and Thelen 2020), Americanists (Guess, Nyhan, and Reifler 2020), and political theorists (Forestal 2020), including in this journal (Collier, Dubal, and Carter 2018; Thelen 2018). Although states also deploy algorithmic governance (Bell 2021), algorithms uniquely power Big Tech’s global scale and influence. Google algorithms use 3.5 billion search inquiries each day (Galloway 2017, 129) to model the likelihood of users clicking on content and then sell this “click-through rate” to advertisers. Google’s profits increased by 3,590% after employing algorithmic pricing (Zuboff 2019, 87), allowing it to buy YouTube, the largest video platform, and expand Android into capturing 72% of the smartphone market (Apple has the rest). Algorithms generate more than six million predictions per second for 2.8 billion users on Facebook (Bucher 2018, 12), the world’s largest social network and media publisher. Of the 68% of Americans who report getting news from social media, their primary source is Facebook (43%), followed

Swati Srivastava  is an assistant professor of political science at Purdue University (srivast70@purdue.edu). Her research on global governance, corporate responsibility, human rights, and constructivism has been published in *International Studies Quarterly*, *International Studies Review*, and the *Oxford Research Encyclopedia of International Studies*. She directs a “Big Tech and Political Responsibility” research lab at Purdue, supported in part by the National Endowment for the Humanities.

doi:10.1017/S1537592721003145

September 2023 | Vol. 21/No. 3 989

© The Author(s), 2021. Published by Cambridge University Press on behalf of the American Political Science Association. This is an Open Access article, distributed under the terms of the Creative Commons Attribution licence (<https://creativecommons.org/licenses/by/4.0/>), which permits unrestricted re-use, distribution, and reproduction in any medium, provided the original work is properly cited.

by YouTube (21%; Shearer and Matsa 2018). When Facebook-owned Instagram and WhatsApp are included, Facebook constitutes 53% of social news pathways. Amazon Web Services (AWS), the largest cloud storage and web-hosting platform, subsidizes its Prime membership used by 64% of US households (Weise 2019). Algorithms thus manifest Big Tech's centralization (Atal 2020, 338) into "highly organized capital backed by vast systems of extraction and logistics" (Crawford 2021, 18–19). Their control of critical bottlenecks transforms Big Tech into arbiters of knowledge, connection, and desire (Zuboff 2019, 127).

Algorithmic governance implicates core IR research in at least two ways. First, algorithms create new private governors "engaged in authoritative decision-making that was previously the prerogative of sovereign states" (Cutler et al. 1999: 16; see Avant, Sell, and Finnemore 2010; Büthe and Mattli 2011; Green 2014; Hall and Biersteker 2002; Stroup and Wong 2017). Big Tech algorithms generate decision environments for both mundane and consequential actions. Google algorithms provide search results for local barbers and mail-in voting instructions; they autoplay recommended YouTube videos on cooking and QAnon. Facebook algorithms sort News Feed content visibility for cat memes and COVID-19 vaccines; they nudge users into joining groups to share knitting patterns and organize violent mobs to attack the US Capitol (Tech Transparency Project 2021). YouTube and Facebook algorithms moderate content in real time alongside humans based on expanding "community guidelines." Even Facebook founder Mark Zuckerberg acknowledges, "In a lot of ways Facebook is more like a government than a traditional company. We have this large community of people, and more than other technology companies we're really setting policies" (Foer 2017). Yet, users did not elect Zuckerberg to govern, nor do they have any representation in Big Tech's private governance.

Second, algorithmic governance expands relations between states and corporations (Avant 2005; Goldsmith and Wu 2006; Mikler 2018; Sell 2003; Strange 1996), especially in human rights contexts. States use corporate algorithms: Google assists drone strikes, Facebook embeds in political campaigns, and Amazon partners with law enforcement. Recent scandals involving Facebook include giving virtual megaphones to extremists responsible for repression in the Rohingya genocide, promoting disinformation from Russian agents in the 2016 US election, and allowing the unauthorized sharing of 87 million users' private data with Cambridge Analytica, a voter profiling company used by Trump. But Big Tech also works against states. Facebook suspended Trump indefinitely when he was president for posts it deemed as inciting the Capitol attack, holding him accountable by doing "what legions of politicians, prosecutors and power brokers had tried and failed to do for years" (Roose 2021). (Facebook later

specified a two-year suspension.) Amazon cut off Parler, a right-wing Trump-supporting social network, as did Apple and Google. Big Tech also resists government calls for forced decryption, such as Apple's refusal to unlock the San Bernardino shooter's iPhone. In response, states have called Big Tech "digital gangsters" (Levy 2020, 11) and retaliated using antitrust, privacy, and speech laws. Even German chancellor Angela Merkel called Trump's Facebook suspension "problematic" (Klonick 2021). Algorithms mediate the scope of these oscillating matchups as states become dependent on Big Tech, Big Tech circumvents state overreach, and states curtail Big Tech.

In this agenda-setting article, I urge IR scholars to learn from and contribute to research on algorithmic governance by incorporating Big Tech and their algorithms as timely objects of research. Through mass surveillance and information manipulation, algorithmic governance can contribute to an erosion of public trust in technology and a misinformed citizenry (Zuboff 2019). As academics engage in the problem-definition phase of algorithms, IR research on private authority and state–corporate relations is well positioned to address the international politics of Big Tech and its "world order challenges" (Farrell and Newman 2019, 163). The next sections of this article introduce algorithmic governance, discuss opportunities for IR interventions in analyzing Big Tech's private authority and state–corporate relations, and conclude with avenues for future research.

Algorithmic Governance

Global relations are increasingly undergirded by proprietary and opaque algorithms that organize the world's information and connections. Classification algorithms, in particular, govern by "generating knowledge systems to execute or inform decisions" (Yeung 2018, 507) through automated profiling and predictions. Risk-assessment algorithms related to credit, terrorism, or crime "construct people's identities and reputations by classifying them as risky, associating them with undesirable traits or correlations, or placing them in the same categories as other people who are risky or have undesirable characteristics" (Balkin 2018, 1167). Algorithms use increasingly granular behavioral data that contain not "only what you post online, but whether you use exclamation points or the color saturation of your photos; not just where you walk but the stoop of your shoulders; not just the identity of your face but the emotional states conveyed by your 'microexpressions'; not just what you like but the pattern of likes across engagements" (Zuboff 2020). Classifying individual users as possible spammers or extremists may rely on "high rate of declined friend requests, gender-unbalanced networks, or using certain phrases" (Schwarz 2019, 7). Algorithms are thus comparable to previous technologies, like cartography, that make us more legible and governable (Scott 1998).

But algorithms also differ from what has come before. First, “the speed, scale and ubiquity of the technologies that make algorithmic governance possible are grander” (Danaher et al. 2017, 2). Computer processors are faster and cheaper, as evident when comparing smartphones to the mainframes of decades ago. Moreover, data are non-perishable and nonexcludable, meaning data can be shared many times without “loss of quality or utility” (Yeung and Lodge 2019, 11), unlike oil or other resources. Second, algorithms have shifted from “top-down” designs, “in which a programmer or team of programmers exhaustively defines the ruleset for the algorithm,” to “bottom-up” machine-learning designs “in which the algorithm is given a learning rule and trained on large datasets in order to develop its own rules” (Danaher et al. 2017, 3). Machine-learning algorithms have the “capacity to identify patterns and correlations that cannot be detected by human cognition” (Yeung 2018, 505). Neural networks used for speech recognition by Amazon’s Echo (Alexa) or Google’s automatic translations find patterns in data that humans are unable to discern.

Classification algorithms thus “lower the costs of judgment and therefore increase the amount, rapidity, and spread of judgment, affecting more lives and reputations more quickly, more cheaply, and more pervasively” (Balkin 2018, 1168). As a result, “authority is increasingly expressed algorithmically” (Pasquale 2015, 8). For example, governments use algorithms to ostensibly allocate welfare benefits, combat tax fraud, secure the border, police communities, and prevent terrorism (Katzenbach and Ulbricht 2019, 5). But algorithms themselves are becoming authoritative as a form of rule, becoming “the necessary antidote to subjective decision-making ... within largescale and complex systems” (Caplan and Boyd 2018, 4). Rule by algorithms aims “to pre-empt agency, spontaneity, and risk: to map out possible futures before they happen so objectionable ones can be foreclosed and desirable ones selected” (Andrejevic 2020, 9). Predictive analytics is trusted by ordinary people for organizing contemporary affairs such as hiring employees and identifying romantic partners. Thus, algorithmic governance reflects both the use of algorithms *by* authorities and algorithms *as* authorities.

Researchers have identified privacy concerns with algorithmic governance. Because machine learning optimizes based on inputs, algorithmic governance relies on perpetual surveillance to extract more varied behavioral data: “if everything is known, then all opportunities can be exploited—nothing is missed” (Andrejevic 2020, 7). Google moved beyond search inquiries to read emails in Gmail, hack Wi-Fi routers through Street View cars, and gain access to third-party Android applications. Researchers found “an idle Android phone sent Google 900 data points over the course of 24 hours, including location data” (Amnesty International 2019, 16); 61% of

Android apps “automatically transfer data to Facebook the moment a user opens the app” (Privacy International 2018). Amazon Echo devices listen to audio recordings before the wake word “Alexa” is used, as does Apple with Siri, Google with Google Home, and Facebook with Portal. Google now owns Fitbit, “giving it access to one of the world’s largest databases of activity, exercise and sleep data” (Amnesty International 2019, 14). Facebook’s facial recognition software, DeepFace, is one of the world’s largest facial datasets. Its chief privacy officer admitted, “Can I say that we will never use facial recognition technology for any other purposes [other than suggesting who to tag in photos]? Absolutely not” (Oreskovic 2013). Facebook can also reportedly “eavesdrop on ambient noise, picked up on your phone’s microphone” (Galloway 2017, 103–4).

Surveillance is not just limited to users. Facebook’s Like and Share buttons place tracking cookies on more than 10 million websites, including two-thirds of the thousand most-visited websites, thereby extending surveillance to non-users. Amazon has launched Sidewalk, a mesh Wi-Fi network to connect devices, including its Ring video doorbells: “If you have enough Ring doorbell cameras on your block, it doesn’t matter if you bought one or not; you’re being monitored and, down the road, perhaps your device is pinging them” (Warzel 2019). Big Tech’s surveillance imperatives mean there is a “fast-growing abyss between what we know and what is known about us” (Zuboff 2020). The tremendous “capital required to build AI at scale” suggests that algorithmic governance is “designed to serve existing dominant interests” (Crawford 2021, 8).

Algorithmic governance may also exacerbate bias and discrimination based on protected categories like race or gender. Ruha Benjamin (2019, 12–13) identifies a “New Jim Code” through which developers “encode judgments into technical systems but claim that the racist results of their designs are entirely exterior to the encoding process.” Studies find that Google displays more negative image results, including pornographic images, for Black women and girls than for white counterparts (Noble 2018) and shows ads for highly paid jobs to men more than women (Ananny and Crawford 2018, 977). Amazon’s recruitment algorithm scored applicants based on resumes of men “over a ten-year period and downgraded applications that listed women’s colleges or terms such as ‘women’s chess club’” (Benjamin 2019, 143). Facebook’s content-moderation algorithms are said to “protect white men from hate speech but not Black children” (Angwin and Grassegger 2017). YouTube algorithms had problematic “autocomplete results or racist image tagging systems” (Gorwa 2019, 859).

In addition to having a discriminatory impact based on protected categories, algorithmic governance may “lead to differentiation among nonprotected groups in a way that

disproportionately affects communities with certain attributes (such as lower socioeconomic status)” (Lynskey 2018, 178). The US Federal Trade Commission acknowledged that algorithmic governance “can injure the economic stability and civil rights of the poor, such as when they are targeted for predatory financial products, charged more for goods and services online, or profiled in ways that limit their employment and educational opportunities” (182). Treating “people as risky or otherwise undesirable [that] impose[s] unjustified burdens and hardships on populations, and reinforce[s] existing inequalities” is a form of “algorithmic nuisance” (Balkin 2018, 1167). Yet, regulations ignore these potential harms. For example, the US Department of Housing and Urban Development passed a rule in 2020 that would “create a complete defense to a prima facie case of housing discrimination when the defendant uses an industry-standard algorithmic model to make its housing decisions” (Crawford and Schultz 2019, 1971–72). The rule insulates against discrimination liability when using algorithmic governance.

In sum, machine-learning algorithms classifying social attributes are used to automate governance decisions for private and public purposes, with implications for privacy, bias, and discrimination. As algorithms propel technology firms to global dominance, it is important to place the possibilities and pitfalls of algorithmic governance in a wider context to capture the politics of Big Tech; the consequences of algorithmic harms are magnified as Big Tech assumes a larger political role in governance and as a state partner and interlocutor. In the remainder of this article, I argue that IR is uniquely situated to analyze algorithmic governance’s political significance in research streams on private authority and state–corporate relations.

Algorithmic Governance and Entrepreneurial Private Authority

Private authority has received considerable attention in studies on international politics. IR defines private authority as nonstate rulemaking, broadly encompassing agenda setting, norm generation, capacity building, and rule development (Avant, Sell, and Finnemore 2010; Cutler, Haufler, and Porter 1999; Hall and Biersteker 2002) or as more narrowly meaning to “make rules or set standards that others in world politics adopt” (Green 2014, 4; see Büthe and Mattli 2011). Private authority is often delegated by states (Avant 2005), as discussed in the next section. However, when private authority is not delegated, it may be established through an “entrepreneurial” process by which “private actors must devise potential ways to govern and then peddle their ideas to those who might comprise the governed” (Green 2014, 34). Examples include private regulators like the International Organization of Standardization (ISO) and international nongovernmental actors (INGOs) such as Amnesty

International. The ISO creates worldwide standards and pushes for their adoption by corporations and governments. Amnesty International advocates for the recognition and implementation of human rights on national and global agendas. The ISO and Amnesty International are not given rule-making authority by states; instead, their governing competence is self-generated in response to perceived global problems. A key aspect of entrepreneurial authority is that private actors must legitimate themselves to the governed (Stroup and Wong 2017). This section characterizes notable features of Big Tech’s algorithmic governance as indicative of entrepreneurial private authority and presents the challenges of legitimation. Companies like PayPal, eBay, and GoDaddy have long policed the internet by using “chokepoints to deter unwanted behavior and target inappropriate content” (Tusikov 2016, 7). Big Tech algorithms add new dynamics and complicate regulation by escalating the scale and scope of governance.

Broadly, Big Tech rules by herding billions of users into artificially curated environments. Herding works by “controlling key elements in a person’s immediate context ... [to enable] remote orchestration of the human situation, foreclosing action alternatives and thus moving behavior along a path of heightened probability” (Zuboff 2019, 294). Facebook’s News Feed herds users through posts based on “creator, popularity, type of post, and date—plus its own ad algorithm” (Galloway 2017, 117). A study tracking archived Facebook profiles found that “people see political content on Facebook not only because of their actual interest in politics, but also because their behaviors and the behaviors of their friends lead to an algorithmic interpretation of their interests—and subsequent categorization—as politically interested” (Thorson et al. 2019, 4). The implication is that “those ‘left behind’ cannot necessarily reassess and redress their previously expressed lack of political interest via new encounters with political content on Facebook” (12). Herding can be weaponized. Facebook confirmed that the Internet Research Agency, a shadowy firm with links to the Kremlin, created 470 pages and profiles and 3,000 pro-Trump ads during the 2016 election. The News Feed algorithm propelled the pages, profiles, and ads to reach more than 126 million Americans, 62,000 of whom pledged to attend “129 rallies and events meant to support Trump, oppose Clinton, and protest mosques around the United States” (Vaidhyanathan 2018, 88). Google and Facebook “can have large impacts on voter behavior in elections by shifting the order of search results and news feeds, influencing up to twenty percent of undecided voters” (Rahman 2018, 1669).

Big Tech rulemaking is also evident in content moderation. It took Facebook 18 months to make “its first permanent hire for content moderation” (Gillespie 2018, 118). Eventually, a short “community standards”

document emerged: “Like, *Hitler? We’re against it. Pants, you need to wear them*” (Levy 2020, 249). The length of these standards has since ballooned to more than 10,000 words. For Gillespie (2018, 22), “how platforms are designed and governed not only makes possible social activity, it calls it into being, gives it shape, and affirms its basic legitimacy as a public contribution.” In addition to monitoring explicit images and violent content, Facebook was forced to deal with online harassment of women and racial minorities, who argued “that the abuses have become so unbearable that platforms have an obligation to intervene” (39). YouTube’s content moderation followed a similar path “from an early system of standards to an intricate system of rules due to (1) the rapid increase in both users and volume of content; (2) the globalization and diversity of the online community; and (3) increased reliance on teams of human moderators with diverse backgrounds” (Klonick 2018, 1635). Facebook and YouTube have since “created private bureaucracies to govern their end-user communities” (Balkin 2018, 1180–81).

Yet critics argue that Big Tech’s algorithmic governance incentivizes “information pollution” (Vaidhyathan 2018, 6) as content providers optimize for the algorithm. In 2014, Facebook introduced “Trending Topics,” using algorithms to promote viral stories on News Feed. Facebook had initially contracted with a group of journalists to oversee Trending Topics. In spring 2016, after pressure from conservatives who accused Facebook of suppressing right-wing content, Facebook fired the human moderators and turned over Trending Topics to algorithms entirely (Levy 2020, 340–42). By August 2016, Trending Topics was boosting visibility without accounting for its reliability. Three days before the 2016 election, BuzzFeed reported that 140 pro-Trump fake news websites, all registered in Macedonia, were trending on Facebook and generated “more engagement than those from mainstream media sources” (Marwick and Lewis 2017, 21). After the election, the “fake news” problem entered mainstream discourse (and was weaponized by Trump against critical press).

But algorithms pollute information streams in other ways than providing misinformation. For one, they generate “information overload [by facilitating] the rapidity of dissemination of information, fake or otherwise. In an instant, stories can be shared, whether or not they have been read” (Cooke 2017, 214). In addition, to capture clicks “long-standing news outlets must construct their content with algorithmic and data-centric intermediaries in mind” (Caplan and Boyd 2018, 1). Clickbait and headline skimming do not cultivate an engaged democratic public that must confront complex structural problems (Marichal 2012; Vaidhyathan 2018).

IR can more precisely identify the political harms resulting from Big Tech’s algorithmic governance that go beyond herding and information pollution. Accepting

the status of Big Tech as a private authority means that there must be consent of the governed for it to be legitimate. The IR literature defines legitimacy as “the normative belief by an actor that a rule or institution ought to be obeyed” (Hurd 1999, 381). In global governance, “as long as there is consent and social recognition, an actor—even a private actor—can be accorded the rights, the legitimacy, and the responsibility of an authority” (Hall and Biersteker 2002, 204). There are many sources of nonstate legitimacy, such as “(1) the perceived expertise of the participants; (2) historical practice that renders such exercise of authority acceptable and appropriate; (3) or an explicit or implicit grant of power by states” (Cutler, Haufler, and Porter 1999, 5). Because legitimacy is “earned rather than conferred, it must be constantly justified and defended” (Lake 2013, 111). These justifications are part of the legitimation process, which requires “internalization by the actor of an external standard” (Hurd 1999, 388). Given that it is difficult to observe internalization, scholars operationalize the social recognition of legitimate rule through “implicit or explicit support of parties who occupy higher, equal, or lower positions” (Johnson, Dowd, and Ridgeway 2006, 72). For instance, legitimating the authority of leading INGOs necessitates acquiring deference from states, corporations, and peers (Stroup and Wong 2017, 22).

Big Tech is assuming greater entrepreneurial private authority, but its degree of legitimation falls short of IR standards. In particular, Big Tech betrays conceptions of being “an authority” and “in authority” (Stroup and Wong 2017, 8). Private actors are regarded as being *an* authority based on their expertise, such as scientists or INGOs. Yet, Big Tech’s assertion of private authority exceeds their expertise. Facebook is *not* an expert on regulating speech, much less in all the countries it operates, which Zuckerberg acknowledges: “The core job of what we do is building products that help people connect and communicate. It’s actually quite different from the work of governing a community” (Klonick 2021). Private actors may also be *in* authority, typically as a result of state delegation or, more tenuously, through entrepreneurial consent. But no one asked Big Tech to govern, nor can its governance easily be dispensed with in the absence of consent. The scramble for legitimation has been noted by the companies themselves as they confront their new public responsibilities. Zuckerberg (2018) admitted to Congress after the Cambridge Analytica scandal, “We didn’t take a broad enough view of our responsibility, and that was a big mistake.”

IR can play an important role in specifying what Big Tech’s broader responsibility should look like. Big Tech fits uneasily within international corporate responsibility frameworks. The landmark 2011 United Nations *Guiding Principles on Business and Human Rights* assert that companies have obligations to conduct human rights due

diligence and enact relevant remedies (Srivastava 2020). But the extent of due diligence and remedies remains underspecified. Furthermore, the *Guiding Principles* assume that “while corporations may be considered ‘organs of society,’ they are specialized economic organs, not democratic public interest institutions. As such, their responsibilities cannot and should not simply mirror the duties of states” (A/HRC/8/5, Section 3, para 53). In domestic contexts, legal scholars have challenged the state/nonstate distinction to model algorithmic accountability on “public utility regulation,” which considers Big Tech as a vital public infrastructure providing “foundational goods and services on which the rest of society depend[s]”; these scholars instead describe the need to impose special obligations on Big Tech to ensure access and nondiscrimination (Rahman 2018, 1639). Another “state action” approach proposes that companies who contract with the state could be deemed accountable for constitutional violations, as has been acknowledged for private physicians in prisons (Crawford and Schultz 2019, 1962). International conceptions of corporate responsibility must similarly evolve to reckon with the global scale and scope of Big Tech authority.

Others advocate stronger corporate-initiated regulation of Big Tech. As providers of a “public good,” Big Tech companies must “carefully construct an image of a responsiveness and attentiveness primarily concerned with responding to its user community, much like politicians must do with their constituents” (Marichal 2012, 46). Thus, Big Tech should “create and apply norms, and settle disputes among their end-users” (Balkin 2018, 1194; Klonick 2018). If political talk is characterized as “a common-pool resource essential to the healthy function of any democracy,” then “social media platforms have an obligation to their users, and their users to one another, to practice that talk agonistically, rather than antagonistically” (Collins, Marichal, and Neve 2020, 415). Users-as-constituents may expect the following from their tech overlords: (1) obligations of transparency, notice, and fair procedures; (2) the offer of reasoned explanations for decisions or changes of policy; (3) the ability of end-users to complain about the conduct of the institution and demand reforms; and (4) the ability of end-users to participate, even in the most limited ways, in the governance of the institution” (Balkin 2018, 1198).

One example of Big Tech-initiated regulation is Facebook’s Content Oversight Board, which became operational in October 2020. The mission of the 40-person board is to develop private case law, especially in hate speech, that “real courts would eventually cite” (Klonick 2021). Board members include a former Danish prime minister, human rights lawyers, journalists, and a Nobel laureate. In creating the board, Facebook leadership recognized the importance of public legitimacy: “At the end of the day you can build all the things, but you just have to

have enough people that believe in order to make it real” (Klonick 2021). The board’s global scope appears vast; it supports 18 languages, three times the UN’s 6. Yet, its mandate to counter algorithmic harms is narrow. For the first seven months, users could only appeal content take-downs, not content left up—which made it difficult to combat misinformation. Users still cannot challenge issues related to advertising or algorithms. Moreover, the board only reviews a tiny fraction of the 200,000 posts eligible for appeal daily from automated and human moderation (Klonick 2021), issuing 18 decisions thus far. The highest-profile case concerned the Trump suspension. Facebook referred the case to the board after Trump left office (per the bylaws, Trump could not appeal the suspension himself). In May 2021, it upheld the suspension but admonished Facebook for not specifying its length: “Facebook cannot make up the rules as it goes, and anyone concerned about its power should be concerned about allowing this. Having clear rules that apply to all users and Facebook is essential for ensuring the company treats users fairly” (Oversight Board 2021).

Even if private governors provide clear rules and due process, algorithmic governance complicates the legitimation process in three ways by. First, the opacity of algorithms makes it difficult to know precisely when one is being influenced by algorithms and then to identify specific harms. Welfare claimants have “very little understanding of exactly how and why the AI system had reduced their benefits, and even less of an opportunity to hold accountable the private technology vendors who were primarily responsible for the harm” (Crawford and Schultz 2019, 1951–52). Government agencies that contract algorithms are similarly clueless about “how the AI software code had been written, where the mistakes were made, what data had been used to train and test it, or what means were required to mitigate concerns” (1968). The surveilled and manipulated “lack any realistic prospect of peering into, let alone comprehending, the algorithmic black boxes” (Yeung 2018, 518). When users are unaware that they are being governed, any deference from them is not based on proper internalization, which is key to legitimation.

Second, algorithms may also be opaque to their designers, thereby complicating human rights due diligence assessments recommended by those advocating corporate-initiated regulation (Kaye 2018). Unsupervised machine-learning algorithms are “not able to tell programmers exactly why they produce the outputs they do” (Donaher 2016, 255). In AI systems, there are distinctions between “human-in-the-loop” with full human command, “human-on-the-loop” with possible human override, and “human-out-of-the-loop” with no human oversight (Citron and Pasquale 2014). These distinctions collapse as more deference to algorithms leads to “systems that are far more complex and outside the upper limits of

human reason” (Donaher 2016, 253). There are “almost limitless domains in which algorithmic systems may be shown to ‘outperform’ humans on a very wide range of tasks across multiple social domains” (Yeung and Lodge 2019, 12). Thus, algorithms represent a “black box” in two ways: as “a recording device, like the data-monitoring systems in planes, trains, and cars” and “a system whose workings are mysterious; we can observe its inputs and outputs, but we cannot tell how one becomes the other” (Pasquale 2015, 3).

Third, it is a slippery slope from presenting algorithms as black boxes into asserting that *only* Big Tech can hold itself accountable. In 2014, a new “right to be forgotten” emerged when the European Court of Justice demanded that Google Spain delink embarrassing search results. Yet the Court also acknowledged that Google alone is capable of enforcing this right (Balkin 2018, 1180). Google subsequently manipulated the framing of this right in public discourse, including by promoting itself as a “truth engine” (Powles 2015, 591). Thus, even though advocating transparency is important, algorithms raise a bigger challenge: “transactions that are too complex to explain to outsiders may well be too complex to be allowed to exist” (Pasquale 2015, 16). Could we properly legitimate Big Tech’s governance as a private authority when facing monopolistic expertise with no obvious countervailing force? Or is Big Tech governance akin to coercion, seen as “asymmetrical physical power among agents, where this asymmetry is applied to changing the behavior of the weaker agent” (Hurd 1999, 383)?

The self-authorizing nature of Big Tech algorithmic governance is difficult to legitimate using existing conceptions, presenting an opening for private authority scholars in IR to intervene by theorizing new kinds of corporate international responsibility, assessing the ideologies and legitimation claims of Big Tech, surveying the deference that constitutes Big Tech’s entrepreneurial authority, and developing tools for evaluating corporate-initiated regulation by priming users to orient their identities as constituents, not consumers.

Algorithmic Governance and State–Corporate Relations

Algorithmic governance also offers new opportunities for IR research to explore the implications of globalized corporate infrastructures for state power (Strange 1996). Eschewing earlier notions of a globalized but decentralized, self-governing, “borderless” digital sphere, IR scholars have noted the “effects of coercive governmental force on local persons, firms, and equipment” (Goldsmith and Wu 2006, 180). In addition, they argue that the globalized landscape features “centralized, hierarchical corporations territorialized in a handful of powerful states” (Atal 2020, 345). Recent studies move beyond a “states versus markets” view to assert instead that “there are large,

powerful global corporations and large, powerful states, and they may be acting together rather than in opposition to one another” (Mikler 2018, 16). The aim is thus to understand complex relationships between states and corporations that include both collaboration and contestation. Within this context, Big Tech may be conceived as “simultaneously challenging and reshaping the traditional role of states while also being used to shore up and expand older forms of geopolitical power” (Crawford 2021, 186). This section explores three kinds of state–corporate relations made visible in algorithmic governance: interdependence (states contracting with Big Tech), circumvention (Big Tech pushing against state overreach), and curtailment (states regulating Big Tech).

In interdependent relationships, states delegate internet governance to corporations on matters related to censorship, surveillance, copyright, and law enforcement (DeNardis 2014, 13). States have come to “rely on censorship and criminalization to shape the online regulatory environment. Broadly worded restrictive laws on ‘extremism,’ blasphemy, defamation, ‘offensive’ speech, ‘false news’ and ‘propaganda’ often serve as pretexts for demanding that companies suppress legitimate discourse” (Kaye 2018, 6). State-delegated content moderation requires “companies to restrict manifestly illegal content such as representations of child sexual abuse, direct and credible threats of harm and incitement to violence” (6). Given the volume of takedown requests, some states have “established specialized government units to refer content to companies for removal” (8). The delegated relationship between states and Big Tech “ranges from direct regulation, to threats, to suggestions that things will go better for infrastructure operators if they cooperate, to negotiations over the terms of cooperation” (Balkin 2018, 1180).

Algorithmic governance is also used for national security purposes, contributing to the post–Cold War trend of privatization in international politics (Avant 2005). In 2013, Edward Snowden revealed that Facebook and Google were sharing user data with intelligence agencies in the United States, the United Kingdom, and the Five Eyes alliance comprising those two countries plus Australia, New Zealand, and Canada. Amazon reportedly has more than 2,000 partnerships with US law enforcement agencies, allowing them to use its Ring video doorbell data (Lyon 2021). Google’s image recognition algorithms have helped inform target selection for US drone strikes in the “War on Terror” (Amoore 2020). Facebook helps Pakistan identify blasphemy, Norway police communities, and Russia block pages supporting Putin’s critics. In 2016, Rodrigo Duterte became president of the Philippines after using Facebook to “manufacture and spread false stories, and undermine trust in professional journalists” (Vaidhyanathan 2018, 191). Since then, Duterte’s Facebook vigilantism against suspected drug traffickers has led to the deaths of more than 1,400 people. Apple maintains

data servers for Chinese users in China with no way of stopping the state from accessing them. Amnesty International (2019, 6) warns that “the opportunity to access such data has created a powerful disincentive for governments to regulate corporate surveillance.” IR scholars are concerned about privacy trade-offs in Big Tech solutions to reduce the spread of COVID-19, such as Google and Apple’s contact tracing app for health bureaucracies (Wong 2020). Thus, one outcome of state–Big Tech interdependence is that algorithmic governance may usher in “a world in which large, global, privately-owned platforms become the regulatory agents of nation states” (Balkin 2018, 1207).

In the second type of relationship, Big Tech corporations circumvent state power to champion human rights in particular contexts. Human rights arenas in which coercive governmental force confronts Big Tech include “rights to privacy, religious freedom and belief, opinion and expression, assembly and association, and public participation, among others” (Kaye 2018, 3). States differ in imposing obligations for internet intermediaries regarding freedom of expression, ranging from the United States’ “broad immunity,” Europe and Russia’s “conditional liability,” and China and the Middle East’s “strict liability” (Gillespie 2018, 33). Companies have deployed universal human rights principles to insulate against clashing state interests. Microsoft president Brad Smith (2017) advocates “protecting civilians from nation-state attacks in times of peace” by leveraging Big Tech’s “role as the internet’s first responders” to “commit ourselves to collective action that will make the internet a safer place, affirming a role as a neutral Digital Switzerland that assists customers everywhere and retains the world’s trust.” In this vein, Facebook hired its inaugural director of human rights in 2020 and later released a new corporate human rights policy, including a fund for “human rights defenders.” Facebook referenced the UN *Guiding Principles on Business and Human Rights* and the International Bill of Human Rights in its commitment to challenging states’ forced decryption and what the company considers to be overbroad requests: “The struggle for human rights online will continue to face new challenges as authoritarian governments are increasingly seeking to exert control over the internet and use it as a means of repression. No one company will be perfect, but we will do all we can to live up to the commitments we are making today” (Sissons 2021).

Pushback from Big Tech against states is also evident in the development of “tech ethics.” In 2017, the Pentagon contracted with Google on Project Maven to create “an automated search engine of drone videos to detect and track enemy combatants” (Crawford 2021, 189). More than 3,000 Google employees signed a letter in protest, and the company responded by terminating the contract. After Amazon took over the contract, Google released a

statement of its AI principles, noting it would not pursue collaborations on “weapons or other technologies whose principal purpose or implementation is to cause or directly facilitate injury to people” or on “technologies that gather or use information for surveillance violating internationally accepted norms” (191). Almost 200 Facebook employees demanded an audit in response to company algorithms disproportionately flagging Black and Palestinian activism as problematic (Dwoskin and De Vynck 2021). Whereas these efforts within Big Tech to foreground ethics have originated in a bottom-up fashion from employees, Facebook’s Oversight Board is the most institutionalized form of top-down tech ethics. In the Trump decision, it drew on the UN Commission of Human Rights’ Rabat Plan of Action when recommending that Facebook “resist pressure from governments to silence their political opposition” and when “evaluating political speech from highly influential users, Facebook should rapidly escalate the content moderation process to specialized staff who are familiar with the linguistic and political context” (Oversight Board 2021). But the decision did not clarify what the board would “do when Facebook’s rules conflict with international human rights law,” which is for some “the hardest question” (Douek 2021).

Finally, Big Tech’s algorithmic prowess has mobilized states to curtail corporate power, especially in actions related to antitrust, privacy, and speech. In July 2020, a US congressional hearing presented Big Tech as an existential threat: “Their ability to dictate terms, call the shots, upend entire sectors, and inspire fear, represent the powers of a private government. Our founders would not bow before a king, nor should we bow before the emperors of the online economy” (Cicilline 2020). The Department of Justice has since brought antitrust suits against Google and Facebook while investigating Apple and Amazon. After the Cambridge Analytica scandal, the Federal Trade Commission fined Facebook \$5 billion, the largest amount it ever levied for a privacy violation. The European Union implemented the General Data Protection Regulation (GDPR) in 2018, under which maximum fines for privacy violations can be up to 4% of a company’s global revenue. The GDPR has led to more disclosure in privacy policies and foregrounded opt-out messaging for tracking cookies across the web. In the United States, Big Tech is shielded from speech regulation, because Section 230 of the 1996 Communications Decency Act regards internet platforms as distinct from publishers. But this “intermediary immunity” is currently under threat. Elsewhere, Germany’s 2017 “Network Enforcement” law “makes companies liable for illegal speech propagated via their services” (Gorwa 2019, 855).

Civil society has also launched initiatives to promote “digital rights”: a “range of protections regarding access to the Internet, privacy, transparency regarding how data is used, control over how data is used, democratic

participation in municipal technology decisions and more” (Wylie 2019). The 2018 Toronto Declaration, spearheaded by Amnesty International and Access Now, calls on governments and companies to protect the right to equality and nondiscrimination in AI systems. These activists have allies in Europe, where the GDPR articulates an individual’s “right not to be subject to a decision based solely on automated processing, including profiling” (Article 22.1). This right has broad exceptions for algorithmic governance, including if “necessary for entering into, or performance of, a contract between the data subject and a data controller”; if authorized by law; or if based on “explicit consent.” Still, the framework shifts the burden of algorithmic harm reduction from individuals to companies, rendering it more “effective in practice” (Lynskey 2018, 197). The European Commission also proposed a Digital Services Act in 2020 that would impose additional corporate liability for content moderation and force disclosures of algorithms.

States and Big Tech corporations engage in many collaborative and contentious relations of relevance to international politics. The dynamics of these emerging state–corporate relations require more sustained IR scrutiny. For instance, given that states already find it difficult to oversee delegated authority (Avant 2005), studies should inquire how algorithms make Big Tech partnerships harder to regulate for states. More research is also needed on Big Tech’s traditional state capture through lobbyists (Atal 2020), including in global economic institutions (Sell 2003), and its less traditional cultivation of “a privileged alliance with consumers . . . providing a formidable source of opposition to regulation that threatens the convenience provided by these platforms” (Culpepper and Thelen 2020, 290). Finally, we need systematic assessments of the emergence, diffusion, and effectiveness of public advocacy and regulations regarding Big Tech (Farrell and Newman 2019).

Conclusion

Algorithmic governance, especially but not exclusively expressed in Big Tech, is ripe for examination in IR research. Several IR research streams are especially needed. Researchers in private authority should investigate US tech giants’ strategies and outcomes related to global governance, including in a comparative context with each other and their Chinese counterparts Alibaba, Tencent, Baidu, and Huawei. They should evaluate the ideology underpinning Silicon Valley capitalism and the conditions under which Big Tech legitimation claims are successful. Also needed is analysis of the promises and challenges of creating responsible AI and the role of transnational advocacy networks therein. Scholars of state–corporate relations should study the comparative strength and scope of national regulations in remedying algorithmic harms, along with developments in public and private international law. They should explore Big Tech’s support of and challenge to traditional state

treatments of speech, monopoly, and privacy. Given that China boasts of “AI supremacy” by 2030, scholars should research Big Tech’s impact on US–Sino competition and whether China’s “digital authoritarianism”—evident in its repression of the Uyghurs—portend a divergent model of algorithmic governance or a convergent one for Western democracies. By embarking on this wide-ranging agenda, IR will bolster the interdisciplinary study of algorithmic governance and advance understanding of the international politics of Big Tech.

References

- Amnesty International. 2019. “Surveillance Giants: How the Business Model of Google and Facebook Threatens Human Rights.” <https://www.amnesty.org/download/Documents/POL3014042019ENGLISH.PDF>, accessed February 2, 2021.
- Amoore, Louise. 2020. *Cloud Ethics: Algorithms and the Attributes of Ourselves and Others*. Durham, NC: Duke University Press.
- Ananny, Mike, and Kate Crawford. 2018. “Seeing without Knowing: Limitations of the Transparency Ideal and Its Application to Algorithmic Accountability.” *New Media & Society* 20 (3): 973–89.
- Andrejevic, Mark. 2020. *Automated Media*. London: Routledge.
- Angwin, Julia and Hannes, Grassegger. 2017. “Facebook’s Secret Censorship Rules Protect White Men from Hate Speech but not Black Children.” *ProPublica*, June 28.
- Atal, Maha Rafi. 2020. “The Janus Faces of Silicon Valley.” *Review of International Political Economy* 28 (2): 336–50.
- Avant, Deborah. 2005. *Market for Force: The Consequences of Privatizing Security*. Cambridge: Cambridge University Press.
- Avant, Deborah, Susan Sell, and Martha Finnemore, eds. 2010. *Who Governs the Globe?* Cambridge: Cambridge University Press.
- Balkin, Jack. 2018. “Free Speech in an Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation.” *UC Davis Law Review* 51: 1149–1210.
- Bell, Bernard. 2021. “Replacing Bureaucrats with Automated Sorcerers?” *Daedalus* 150 (3): 89–103.
- Benjamin, Ruha. 2019. *Race after Technology: Abolitionist Tools for the New Jim Code*. Cambridge: Polity.
- Bucher, Taina. 2018. *If... Then: Algorithmic Power and Politics*. Oxford: Oxford University Press.
- Büthe, Tim, and Walter Mattli. 2011. *The New Global Rulers: The Privatization of Regulation in the World Economy*. Princeton: Princeton University Press.
- Caplan, Robyn, and danah boyd. 2018. “Isomorphism through Algorithms: Institutional Dependencies in the Case of Facebook.” *Big Data & Society* 5 (1): 1–12.

- Cicilline, David. 2020. "Opening Statement." In *Online Platforms and Market Power, Part 6 Hearing before U.S. House of Representatives*, July 29.
- Citron, Danielle, and Frank Pasquale. 2014. "The Scored Society: Due Process for Automated Predictions." *Washington Law Review* 89 (1): 1–33.
- Collins, Brian, José Marichal, and Richard Neve. 2020. "The Social Media Commons: Public Sphere, Agonism, and Algorithmic Obligation." *Journal of Information Technology and Politics* 17 (4): 409–25.
- Collier, Ruth, V. B. Dubal, and Christopher Carter. 2018. "Disrupting Regulation, Regulating Disruption: The Politics of Uber in the United States." *Perspectives on Politics* 16 (4): 919–37.
- Cooke, Nicole. 2017. "Posttruth, Truthiness, and Alternative Facts: Information Behavior and Critical Information Consumption for a New Age." *Library Quarterly* 87 (3): 211–21.
- Crawford, Kate. 2021. *Atlas of AI: Power, Politics, and the Planetary Costs of Artificial Intelligence*. New Haven, CT: Yale University Press.
- Crawford, Kate, and Jason Schultz. 2019. "AI Systems as State Actors." *Columbia Law Review* 119 (7): 1941–72.
- Culpepper, Pepper, and Kathleen Thelen. 2020. "Are We All Amazon Primed? Consumers and the Politics of Platform Power." *Comparative Political Studies* 53 (2): 288–318.
- Cutler, A. Claire, Virginia Haufler, and Tony Porter, eds. 1999. *Private Authority and International Affairs*. Albany: State University of New York Press.
- Dafoe, Allan. 2018. "AI Governance: A Research Agenda." Centre for the Governance of AI. <https://www.fhi.ox.ac.uk/wp-content/uploads/GovAI-Agenda.pdf>, accessed March 17, 2021.
- Danaher, John, Michael Hogan, Chris Noone, et al. 2017. "Algorithmic Governance: Developing a Research Agenda through the Power of Collective Intelligence." *Big Data & Society* doi: 10.1177/2053951717726554.
- DeNardis, Laura. 2014. *The Global War for Internet Governance*. New Haven, CT: Yale University Press.
- Donaher, John. 2016. "The Threat of Algocracy: Reality, Resistance and Accommodation." *Philosophy & Technology* 29: 245–68.
- Douek, Evelyn. 2021. "It's Not Over: The Oversight Board's Trump Decision Is just the Start." *Lawfare*, May 5.
- Dwoskin, Elizabeth, and Gerrit De Vynck. 2021. "Facebook's AI Treats Palestinian Activists like It Treats American Black Activists. It Blocks Them." *Washington Post*, May 28.
- Farrell, Henry, and Abraham Newman. 2019. *Of Privacy and Power: The Transatlantic Struggle over Freedom and Security*. Princeton: Princeton University Press.
- Foer, Franklin. 2017. "Facebook's War on Free Will." *The Guardian*, September 19.
- Forestal, Jennifer. 2020. "Beyond Gatekeeping: Propaganda, Democracy, and the Organization of Digital Publics." *Journal of Politics*. doi: 10.1086/709300.
- Galloway, Scott. 2017. *The Four: The Hidden DNA of Amazon, Apple, Facebook, and Google*. New York: Portfolio/Penguin.
- Gillespie, Tarleton. 2018. *Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions that Shape Social Media*. New Haven, CT: Yale University Press.
- Green, Jessica. 2014. *Rethinking Private Authority: Agents and Entrepreneurs in Global Environmental Governance*. Princeton: Princeton University Press.
- Goldsmith, Jack, and Tim Wu. 2006. *Who Controls the Internet? Illusions of a Borderless World*. New York: Oxford University Press.
- Gorwa, Robert. 2019. "What Is Platform Governance?" *Information, Communication and Society* 24 (6): 854–71.
- Guess, Andrew, Brendan Nyhan, and Jason Reifler. 2020. "Exposure to Untrustworthy Websites in the 2016 U.S. Election." *Nature Human Behavior* 4: 472–81.
- Hall, Rodney, and Thomas Biersteker, eds. 2002. *The Emergence of Private Authority in Global Governance*. Cambridge: Cambridge University Press.
- Hurd, Ian. 1999. "Legitimacy and Authority in International Politics." *International Organization* 53 (2): 379–408.
- Johnson, Cathryn, Timothy Dowd, and Cecelia Ridgeway. 2006. "Legitimacy as a Social Process." *Annual Review of Sociology* 32: 53–78.
- Just, Natascha, and Michael Latzer. 2017. "Governance by Algorithms: Reality Construction by Algorithmic Selection on the Internet." *Media, Culture & Society* 39 (2): 238–58.
- Katzenbach, Christian, and Lena Ulbricht. 2019. "Algorithmic Governance." *Internet Policy Review* 8 (4). doi: 10.14763/2019.4.1424.
- Kaye, David. 2018. "A Human Rights Approach to Platform Content Regulation." <https://freedex.org/a-human-rights-approach-to-platform-content-regulation>, accessed February 2, 2021.
- Klonick, Kate. 2018. "The New Governors: The People, Rules, and Processes Governing Online Speech." *Harvard Law Review* 131: 1598–670.
- Klonick, Kate. 2021. "Inside the Making of Facebook's Supreme Court." *New Yorker*, February 12.
- Lake, David. 2013. "Legitimizing Power: The Domestic Politics of U.S. International Hierarchy." *International Security* 38 (2): 74–111.

- Levy, Steven. 2020. *Facebook: The Inside Story*. New York: Blue Rider Press.
- Lynskey, Orla. 2018. "The Power of Providence: The Role of Platforms in Leveraging the Legibility of Users to Accentuate Inequality." In *Digital Dominance: The Power of Google, Amazon, Facebook, and Apple*, eds. Martin Moore and Damien Tambini, 176–201. Oxford: Oxford University Press.
- Lyon, Kim. 2021. "Amazon's Ring Now Reportedly Partners with More than 2,000 U.S. Police and Fire Departments." *The Verge*, January 31.
- Marichal, José. 2012. *Facebook Democracy: The Architecture of Disclosure and the Threat to Public Life*. Burlington: Ashgate.
- Marwick, Alice, and Rebecca Lewis. 2017. "Media Manipulation and Disinformation Online." *Data & Society*. <https://datasociety.net/library/media-manipulation-and-disinfo-online>, accessed February 2, 2021.
- Mikler, John. 2018. *The Political Power of Global Corporations*. Cambridge: Polity.
- Noble, Safiya. 2018. *Algorithms of Oppression: How Search Engines Reinforce Racism*. New York: NYU Press.
- Oreskovic, Alexei. 2013. "Facebook Considers Adding Profile Photos to Facial Recognition." *Reuters*, August 29.
- Oversight Board. 2021. Case 2021-001-FB-FBR. <https://oversightboard.com/decision/FB-691QAMHJ/>, accessed May 28, 2021.
- Pasquale, Frank. 2015. *The Black Box Society: The Secret Algorithms that Control Money and Information*. Cambridge, MA: Harvard University Press.
- Powles, Julia. 2015. "The Case that Won't be Forgotten." *Loyola University Chicago Law Review* 47 (2): 583–615.
- Privacy International. 2018. *How Apps on Android Share Data with Facebook*, December 29. London: Privacy International.
- Rahman, Sabeel. 2018. "The New Utilities: Private Power, Social Infrastructure, and the Revival of the Public Utility Concept." *Cardozo Law Review* 39: 1621–89.
- Roose, Kevin. 2021. "In Pulling Trump's Megaphone, Twitter Shows Where Power Now Lies," *New York Times*, January 9.
- Schwarz, Ori. 2019. "Facebook Rules: Structures of Governance in Digital Capitalism and the Control of Generalized Social Capital." *Theory, Culture & Society* 36 (4): 117–41.
- Scott, James C. 1998. *Seeing like a State: How Certain Schemes to Improve the Human Condition Have Failed*. New Haven: Yale University Press.
- Sell, Susan. 2003. *Private Power, Public Law: The Globalization of Intellectual Property Rights*. Cambridge: Cambridge University Press.
- Shearer, Elisa, and Katerina Eva Matsa. 2018. *News Use across Social Media Platforms*, September 10. Washington, DC: Pew Research Center.
- Sissons, Miranda. 2021. "Our Commitment to Human Rights." *Facebook*, March 16. <https://about.fb.com/news/2021/03/our-commitment-to-human-rights/>, accessed May 28, 2021.
- Smith, Brad. 2017. "The Need for a Digital Geneva Convention." *Microsoft*, February 14. <https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/>, accessed September 27, 2021.
- Srivastava, Swati. 2020. "Corporate Responsibility." *Oxford Research Encyclopedia of International Studies*. doi: 10.1093/acrefore/9780190846626.013.582.
- Strange, Susan. 1996. *The Retreat of the State: The Diffusion of Power in the World Economy*. Cambridge: Cambridge University Press.
- Stroup, Sarah, and Wendy Wong. 2017. *The Authority Trap: Strategic Choices of International NGOs*. Ithaca, NY: Cornell University Press.
- Tech Transparency Project. 2021. *Capitol Attack Was Months in the Making on Facebook*, January 19. Washington, DC: Campaign for Accountability.
- Thelen, Kathleen. 2018. "Regulating Uber: The Politics of the Platform Economy in Europe and the United States." *Perspectives on Politics* 16 (4): 938–53.
- Thorson, Kjerstin, Kelley Cotter, Mel Medeiros, and Chankyung Pak. 2019. "Algorithmic Inference, Political Interest, and Exposure to News and Politics on Facebook." *Information, Communication & Society*. doi: 10.1080/1369118X.2019.1642934.
- Tusikov, Natasha. 2016. *Chokepoints: Global Private Regulation on the Internet*. Berkeley: University of California Press.
- Vaidhyanathan, Siva. 2018. *Antisocial Media: How Facebook Disconnects Us and Undermines Democracy*. New York: Oxford University Press.
- Warzel, Charlie. 2019. "Amazon Wants to Surveil Your Dog." *New York Times*, October 4.
- Weise, Karen. 2019. "Prime Power: How Amazon Squeezes the Businesses behind Its Store." *New York Times*, December 20.
- Wong, Wendy. 2020. "Technology Threatens Human Rights in the Coronavirus Fight." *The Conversation*, May 7.
- Wylie, Bianca. 2019. "Why We Need Data Rights: 'Not Everything about Us Should Be for Sale.'" *Financial Post*, February 1.

Yeung, Karen. 2018. "Algorithmic Regulation: A Critical Interrogation." *Regulation & Governance* 12 (4): 505–23.

Yeung, Karen, and Martin Lodge, eds. 2019. *Algorithmic Regulation*. New York: Oxford University Press.

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

Zuboff, Shoshana. 2020. "You are Now Remotely Controlled." *New York Times*, January 24.

Zuckerberg, Mark. 2018. *Facebook, Social Media Privacy, and the Use and Abuse of Data: Joint Hearing Before the S. Comm. on the Judiciary and the S. Comm. on Commerce, Science and Transportation, 115th Cong.* (2018) (statement of Mark Zuckerberg, CEO of Facebook).