2019 Report

AINOW

December 2019

AUTHORS AND CONTRIBUTORS

Kate Crawford, AI Now Institute, New York University, Microsoft Research
Roel Dobbe, AI Now Institute, New York University
Theodora Dryer, AI Now Institute, New York University
Genevieve Fried, AI Now Institute, New York University
Ben Green, AI Now Institute, New York University
Elizabeth Kaziunas, AI Now Institute, New York University
Amba Kak, AI Now Institute, New York University
Varoon Mathur, AI Now Institute, New York University
Erin McElroy, AI Now Institute, New York University
Andrea Nill Sánchez, AI Now Institute, New York University
Deborah Raji, AI Now Institute, New York University
Joy Lisi Rankin, AI Now Institute, New York University
Rashida Richardson, AI Now Institute, New York University
Jason Schultz, AI Now Institute, New York University School of Law
Sarah Myers West, AI Now Institute, New York University
Meredith Whittaker, AI Now Institute, New York University

With research assistance from Alejandro Calcaño Bertorelli and Joan Greenbaum (AI Now Institute, New York University)

DECEMBER 2019

Cite as: Crawford, Kate, Roel Dobbe, Theodora Dryer, Genevieve Fried, Ben Green, Elizabeth Kaziunas, Amba Kak, Varoon Mathur, Erin McElroy, Andrea Nill Sánchez, Deborah Raji, Joy Lisi Rankin, Rashida Richardson, Jason Schultz, Sarah Myers West, and Meredith Whittaker. *AI Now 2019 Report*. New York: AI Now Institute, 2019, https://ainowinstitute.org/AI_Now_2019_Report.html.

TABLE OF CONTENTS

ABOUT THE AI NOW INSTITUTE

The AI Now Institute at New York University is an interdisciplinary research institute dedicated to understanding the social implications of AI technologies. It is the first university research center focused specifically on AI's social significance. Founded by Kate Crawford and Meredith Whittaker in 2017, AI Now is one of the few women-led AI institutes in the world.

AI Now works with a broad coalition of stakeholders, including academic researchers, industry, civil society, policymakers, and impacted communities, to understand and address issues raised by the rapid introduction of AI across core social domains. AI Now produces interdisciplinary research to help ensure that AI systems are accountable to the communities and contexts they are meant to serve, and that they are applied in ways that promote justice and equity. The Institute's current research agenda focuses on four core areas: bias and inclusion, rights and liberties, labor and automation, and safety and critical infrastructure.

Our most recent publications include:

- **Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice**, an article on how "dirty-policing" practices and policies shape the environment and the methodology by which data is created, raising the risk of creating inaccurate, skewed, or systematically biased "dirty data."
- **Anatomy of an AI System**, a large-scale map and longform essay produced in partnership with SHARE Lab, which investigates the human labor, data, and planetary resources required to operate an Amazon Echo.
- **Discriminating Systems: Gender, Race, and Power in AI**, a report that examines how discrimination and inequality in the AI sector are replicated in AI technology and offers recommendations for change.
- **Disability, Bias, and AI**, drawing on a wealth of research from disability advocates and scholars, this report examines what disability studies and activism can tell us about the risks and possibilities of AI.
- **Excavating AI**, an essay on the politics of images in machine learning training sets.
- **Litigating Algorithms 2019 US Report: New Challenges to Government Use of Algorithmic Decision Systems**, our second major report assessing recent court cases focused on government use of algorithms.

We also host expert workshops and public events on a wide range of topics. Our annual public **AI Now Symposium** convenes leaders from academia, industry, government, and civil society to examine the biggest challenges we face as AI moves into our everyday lives. Recordings of the program are available online.

More information is available at **ainowinstitute.org**

RECOMMENDATIONS

1. **Regulators should ban the use of affect recognition in important decisions that impact people's lives and access to opportunities. Until then, AI companies should stop deploying it.** Given the contested scientific foundations of affect recognition technology—a subclass of facial recognition that claims to detect things such as personality, emotions, mental health, and other interior states—it should not be allowed to play a role in important decisions about human lives, such as who is interviewed or hired for a job, the price of insurance, patient pain assessments, or student performance in school. Building on last year's recommendation for stringent regulation, governments should specifically prohibit use of affect recognition in high-stakes decision-making processes.

2. **Government and business should halt all use of facial recognition in sensitive social and political contexts until the risks are fully studied and adequate regulations are in place.** In 2019, there has been a rapid expansion of facial recognition in many domains. Yet there is mounting evidence that this technology causes serious harm, most often to people of color and the poor. There should be a moratorium on all uses of facial recognition in sensitive social and political domains—including surveillance, policing, education, and employment—where facial recognition poses risks and consequences that cannot be remedied retroactively. Lawmakers must supplement a moratorium with (1) transparency requirements that allow researchers, policymakers, and communities to assess and understand the best possible approach to restricting and regulating facial recognition; and (2) protections that provide the communities on whom such technologies are used with the power to make their own evaluations and rejections of its deployment.

3. **The AI industry needs to make significant structural changes to address systemic racism, misogyny, and lack of diversity.** The AI industry is strikingly homogeneous, due in large part to its treatment of women, people of color, gender minorities, and other underrepresented groups. To begin addressing this problem, more information should be shared publicly about compensation levels, response rates to harassment and discrimination, and hiring practices. It also requires ending pay and opportunity inequality and providing real incentives for executives to create, promote, and protect inclusive workplaces. Finally, any measures taken should address the two-tiered workforce, in which many of the people of color at tech companies work as undercompensated and vulnerable temporary workers, vendors, or contractors.

4. **AI bias research should move beyond technical fixes to address the broader politics and consequences of AI's use.** Research on AI bias and fairness has begun to expand beyond technical solutions that target statistical parity, but there needs to be a much more

rigorous examination of AI's politics and consequences, including close attention to AI's classification practices and harms. This will require that the field center "non-technical" disciplines whose work traditionally examines such issues, including science and technology studies, critical race studies, disability studies, and other disciplines keenly attuned to social context, including how difference is constructed, the work of classification, and its consequences.

5. **Governments should mandate public disclosure of the AI industry's climate impact.** Given the significant environmental impacts of AI development, as well as the concentration of power in the AI industry, it is important for governments to ensure that large-scale AI providers disclose the climate costs of AI development to the public. As with similar requirements for the automotive and airline industries, such disclosure helps provide the foundation for more informed collective choices around climate and technology. Disclosure should include notifications that allow developers and researchers to understand the specific climate cost of their use of AI infrastructure. Climate-impact reporting should be separate from any accounting for offsets or other mitigation strategies. In addition, governments should use that data to ensure that AI policies take into account the climate impacts of any proposed AI deployment.

6. **Workers should have the right to contest exploitative and invasive AI—and unions can help.** The introduction of AI-enabled labor-management systems raises significant questions about worker rights and safety. The use of these systems—from Amazon warehouses to Uber and InstaCart—pools power and control in the hands of employers and harms mainly low-wage workers (who are disproportionately people of color) by setting productivity targets linked to chronic injuries, psychological stress, and even death and by imposing unpredictable algorithmic wage cuts that undermine economic stability. Workers deserve the right to contest such determinations, and to collectively agree on workplace standards that are safe, fair, and predictable. Unions have traditionally been an important part of this process, which underscores the need for companies to allow their workers to organize without fear of retaliation.

7. **Tech workers should have the right to know what they are building and to contest unethical or harmful uses of their work.** Over the last two years, organized tech workers and whistleblowers have emerged as a powerful force for AI accountability, exposing secretive contracts and plans for harmful products, from autonomous weapons to tracking-and-surveillance infrastructure. Given the general-purpose nature of most AI technology, the engineers designing and developing a system are often unaware of how it will ultimately be used. An object-recognition model trained to enable aerial surveillance could just as easily be applied to disaster relief as it could to weapons targeting. Too often, decisions about how AI is used are left to sales departments and executives, hidden behind highly confidential contractual agreements that are inaccessible to workers and the public. Companies should ensure that workers are able to track where their work is

being applied, by whom, and to what end. Providing such information enables workers to make ethical choices and gives them power to collectively contest harmful applications.

8. **States should craft expanded biometric privacy laws that regulate both public and private actors.** Biometric data, from DNA to faceprints, is at the core of many harmful AI systems. Over a decade ago, Illinois adopted the Biometric Information Privacy Act (BIPA), which has now become one of the strongest and most effective privacy protections in the United States. BIPA allows individuals to sue for almost any unauthorized collection and use of their biometric data by a private actor, including for surveillance, tracking, and profiling via facial recognition. BIPA also shuts down the gray and black markets that sell data and make it vulnerable to breaches and exploitation. States that adopt BIPA should expand it to include government use, which will mitigate many of biometric AI's harms, especially in parallel with other approaches, such as moratoriums and prohibitions.

9. **Lawmakers need to regulate the integration of public and private surveillance infrastructures.** This year, there was a surge in the integration of privately owned technological infrastructures with public systems, from "smart" cities to property tech to neighborhood surveillance systems such as Amazon's Ring and Rekognition. Large tech companies like Amazon, Microsoft, and Google also pursued major military and surveillance contracts, further enmeshing those interests. Across Asia, Africa, and Latin America, multiple governments continue to roll out biometric ID projects that create the infrastructure for both state and commercial surveillance. Yet few regulatory regimes govern this intersection. We need strong transparency, accountability, and oversight in these areas, such as recent efforts to mandate public disclosure and debate of public-private tech partnerships, contracts, and acquisitions.[1]

10. **Algorithmic Impact Assessments must account for AI's impact on climate, health, and geographical displacement.** Algorithmic Impact Assessments (AIAs)[2] help governments, companies, and communities assess the social implications of AI, and determine whether and how to use AI systems. Those using AIAs should expand them so that in addition to considering issues of bias, discrimination, and due process, the isues of climate, health, and geographical displacement are included.

11. **Machine learning researchers should account for potential risks and harms and better document the origins of their models and data.** Advances in understanding of bias, fairness, and justice in machine learning research make it clear that assessments of risks and harms are imperative. In addition, using new mechanisms for documenting data provenance and the specificities of individual machine learning models should also become standard research practice. Both Model Cards[3] and Datasheets[4] offer useful templates. As a community, machine learning researchers need to embrace these analyses and tools to create an infrastructure that better considers the implications of AI.[5]

12. **Lawmakers should require informed consent for use of any personal data in health-related AI.** The application of AI in healthcare requires greater protections around data. While the informed-consent process that biomedical researchers and healthcare professionals generally employ in clinical settings requires discussion of the risks and benefits involved, affirmative approval before proceeding, and reasonable opportunities to withdraw from the study or treatment, engineers and scientists commonly create training sets by scraping content from whatever public sources are available. In order to ensure a future that does not amplify and reinforce historic injustices and social harms, AI health systems need better informed-consent approaches and more research to understand their implications in light of systemic health inequities, the organizational practices of healthcare, and diverse cultural approaches to health.

EXECUTIVE SUMMARY

In last year's report, we focused on AI's accountability gap, and asked who is responsible when AI systems harm us, and how we might remedy those harms. Lack of accountability emerged as a real and substantial problem—one that governments, companies, and civil society were just beginning to grapple with, even as AI's deployment into sensitive social domains accelerated.

This year we saw a wave of pushback, as community groups, researchers, policymakers, and workers demanded a halt to risky and dangerous AI. AI Now's 2019 report spotlights these growing movements, examining the coalitions involved and the research, arguments, and tactics used. We also examine the specific harms these coalitions are resisting, from AI-enabled management of workers, to algorithmic determinations of benefits and social services, to surveillance and tracking of immigrants and underrepresented communities. What becomes clear is that across diverse domains and contexts, AI is widening inequality, placing information and control in the hands of those who already have power and further disempowering those who don't. The way in which AI is increasing existing power asymmetries forms the core of our analysis, and from this perspective we examine what researchers, advocates, and policymakers can do to meaningfully address this imbalance.

In doing so, the following key themes emerge:

The spread of algorithmic management technology in the workplace is increasing the power asymmetry between workers and employers. AI threatens not only to disproportionately displace lower-wage earners, but also to reduce wages, job security, and other protections for those who need it most.

This year, we've seen the rapid acceleration of algorithmic systems that control everything from interviewing and onboarding, to worker productivity, to wage setting and scheduling. Whether inside Amazon's fulfillment warehouses, behind the wheel of an Uber, or interviewing for their first job out of college, workers are increasingly managed through AI, with few protections or assurances. AI systems used for worker control and management are inevitably optimized to produce benefits for employers, often at great cost to workers. New research also suggests that lower-wage workers, especially workers of color, will face greater harm from labor automation in the years to come, whether from displacement or from the degradation of work, as workers are increasingly tasked with monitoring and tending to automated systems rather than completing the tasks themselves.

Community groups, workers, journalists, and researchers—not corporate AI ethics statements and policies—have been primarily responsible for pressuring tech companies and governments to set guardrails on the use of AI.

Companies, governments, NGOs, and academic institutions continued to dedicate enormous efforts to generating AI ethics principles and statements this year. However, the vast majority of these say very little about implementation, accountability, or how such ethics would be measured and enforced in practice. In parallel, we have seen growing evidence demonstrating a sharp divide between ethics promises and practice. Increasingly, meaningful action toward AI accountability has come from workers, community advocates, and organizers. In many cases, these efforts are not AI-specific, but rather focus on long-standing discriminatory and harmful policies and how AI-enabled technologies amplify such harms. This includes examples such as criminal justice advocates working to halt the use of discriminatory predictive policing tools, tenants-rights groups opposing facial recognition in housing, and a coalition of Latinx activists, tech workers, and students exposing and protesting lucrative tech company contracts with military and border agencies.

Efforts to regulate AI systems are underway, but they are being outpaced by government adoption of AI systems to surveil and control.

This year alone, we have seen numerous proposed laws and regulations targeting AI. In particular, facial recognition continues as the focus of many debates. Last year, AI Now joined calls to severely limit the use of facial recognition. This year, organizers across the US led the charge, successfully campaigning to pass laws banning facial recognition in several cities. Presidential candidate Bernie Sanders even promised a nationwide ban, and members of the United States Congress proposed several bills, including the Commercial Facial Recognition Privacy Act of 2019, the Facial Recognition Technology Warrant Act, and the No Biometric Barriers Act of 2019. Outside the US, there is litigation over use of the technology by UK police, rulings under GDPR in the EU, and the Australian parliament ordering a complete pause on the use of a national face database.

Yet despite growing public concern and regulatory action, the rollout of facial recognition and other risky AI technologies has barely slowed down. So-called “smart city” projects around the world are consolidating power over civic life in the hands of for-profit technology companies, putting them in charge of managing critical resources and information. For example, Google’s Sidewalk Labs project even promoted the creation of a Google-managed citizen credit score as part of its plan for public-private partnerships like Sidewalk Toronto. And Amazon heavily marketed its Ring, an AI-enabled home-surveillance video camera. The company partnered with over 700 police departments, using police as salespeople to convince residents to buy the system. In exchange, law enforcement was granted easier access to Ring surveillance footage. Meanwhile, companies like Amazon, Microsoft, and Google are fighting to be first in line for massive government contracts to grow the use of AI for tracking and surveillance of refugees and

residents, along with the proliferation of biometric identity systems, contributing to the overall surveillance infrastructure run by private tech companies and made available to governments.

AI systems are continuing to amplify race and gender disparities via techniques like affect recognition, which has no sound scientific basis.

Recent research has highlighted the dire lack of diversity within the AI industry, as well as the vast demographic differences between the populations that benefit and profit from AI's efficiency and those that bear the cost of AI's biases and exploitation. The result: outcomes like the sexist Apple Card algorithms that triggered investigations by both the Senate Committee on Finance and the New York State Department of Financial Services. Rather than recognizing the scale and systemic nature of the problem, tech companies have responded to mounting evidence of bias and misuse by primarily focusing on narrow diversity solutions. They have also attempted technical debiasing, working to "fix" algorithms and diversify data sets, even though these approaches have proven insufficient and raise serious privacy and consent concerns. Notably, neither approach addresses underlying structural inequalities. Nor do the approaches address the growing power asymmetry between those who produce and profit from AI and those subjected to AI's applications.

Affect recognition, a subset of facial recognition that claims to "read" our inner emotions by interpreting the micro-expressions on our face, has been a particular focus of growing concern in 2019—not only because it can encode biases, but because it lacks any solid scientific foundation to ensure accurate or even valid results. This was confirmed in 2019 by the largest metastudy to date on the topic.[6] Critics also noted the similarities between the logic of affect recognition, in which personal worth and character are supposedly discernable from physical characteristics, and discredited race science and physiognomy, which was used to claim that biological differences justified social inequality. Yet in spite of this, AI-enabled affect recognition continues to be deployed at scale across environments from classrooms to job interviews, informing sensitive determinations about who is "productive" or who is a "good worker," often without people's knowledge.

Growing investment in and development of AI has profound implications in areas ranging from climate change to the rights of healthcare patients to the future of geopolitics and inequities being reinforced in regions in the global South.

Finally, our report highlights new concerns associated with the development of AI and its effect on areas ranging from climate change to healthcare to geopolitics. Throughout, we note the significant consequences of AI's use and development, and the danger of leaving determinations around these issues in the hands of a small number of individuals and corporations, whose incentives and worldviews are often at odds with the interests of those who bear the consequences of such decisions.

The climate impact of AI development has become a particular area of concern, as recent research demonstrated that creating just one AI model for natural-language processing can emit as much as 600,000 pounds of carbon dioxide. Key concerns have also emerged regarding how algorithmic health-management tools are impacting patient data and well-being, and the lives of those who care for them. The China "AI arms race" narrative also took center stage this year. In this report we examine the way it has been leveraged to paint efforts to regulate and curb harmful AI as "anti-progress," even though such efforts focus on upholding the democratic values the US claims to promote in its relations with China. Finally, there is a need for more research on the locally specific real-world impact of the AI industry on countries in the global South and the ways it reinforces historical inequities in these regions.

As with our previous reports, we present these findings and concerns in the spirit of engagement, and with the hope that we can contribute to a more holistic understanding of AI that centers the perspectives and needs of those most affected, and that shapes technical development and deployment to these ends.

1. THE GROWING PUSHBACK AGAINST HARMFUL AI

1.1 AI, Power, and Control

Through a combination of surveillance, predictive analytics, and integration into workplace systems such as interviewing, human resources, and supervision, employers are implementing algorithmic systems to rank and assess workers, automatically set wages and performance targets, and even fire workers.[7] In almost every case, these systems are optimized from the perspective of business owners and rarely involve or include worker perspectives, needs, or considerations. Most algorithmic management tools, like most algorithmic decision systems, lack meaningful opportunities for workers to understand how the systems work or to contest or change determinations about their livelihood.

Worker Productivity, AI, and "The Rate"

A growing number of employers rely on AI systems to manage workers and set workloads, accruing significant centralized power and control. For example, Amazon uses an AI system that sets performance targets for workers, a so-called "rate." [8] The "rate" is calculated automatically, and changes from day to day. If a worker falls behind, they are subject to disciplinary action. In many warehouses, termination is an automated process (not unlike being "kicked off" a gig-economy platform).[9] According to Abdi Muse, an organizer with Amazon warehouse workers in Minneapolis, if workers fall behind the algorithmically set productivity rate three times in one day, they are fired, however long they may have worked for the company, and irrespective of the personal circumstances that led to their "mistakes."[10] Muse recounts workers deciding between going to the bathroom and maintaining their rate. Many workers in the Amazon warehouse where he organizes are Somali immigrants, whose work at Amazon helps send money home. This pressure is exacerbated by the low wages paid to many warehouse workers. A report from the Economic Roundtable found that in California's Inland Empire, the home to a major Amazon warehouse hub, "86 percent [of Amazon's logistics employees] earn less than the basic living wage... The typical worker had total annual earnings in 2017 of $20,585, which is slightly over half of the living wage."[11]

Amazon isn't the only company using AI to enforce worker productivity. Chris Ramsaroop, a founding member of the organization Justicia for Migrant Workers, documents the integration of tracking and productivity technologies in the agriculture sector in Canada, finding that "surveillance technologies are utilized to regiment workers to determine their pace at work and their production levels, much like what we see in warehouses."[12] When the Philadelphia Marriott Downtown began using an app to give its housekeepers room assignments, workers found the new system sent them zigzagging across a hotel the size of a city block. It reduced their ability to organize their day, making their work more physically demanding.[13] Reporting earlier this year also

revealed that the Children's Hospital of Philadelphia (CHOP) hired outside contractors to assemble and distribute supplies like syringes, gauze, and other essential equipment and used an opaque algorithmic "rate" that set the amount of work. If anything is off, it's "nearly impossible to meet [the rate]," say workers, "if they're understaffed or overstaffed, if it's a holiday, if there's a person who's new and just getting up to speed." And, if workers don't meet their rate, they'll be written up.[14]

CHOP links the practice of hiring contract workers (whose labor is leased by one firm to another) to algorithmically set productivity rates. This mandates a rate of productivity as part of the contractual agreement and enforces that rate through an algorithm, instead of through on-site supervisors.

Such rate-setting systems rely on pervasive worker surveillance to measure how much they are doing. Systems to enable such invasive worker monitoring are becoming more common, including in traditionally "white-collar" working environments. For example, the start-up Humanyze incorporates sensors into employee badges to monitor employee activities, telling employers where workers go, whom they interact with, and how long they stay in a given place. Another company called Workplace Advisor uses heat sensors to achieve a similar aim. And though the usefulness of these products is disputed,[15] they reflect an increasing willingness to engage in invasive surveillance of workers in the name of workplace control and eking out incremental gains in productivity.

Algorithmic Wage Control

Algorithmic worker management and control systems have also had a severe negative impact on wages across the so-called "gig economy." These platforms treat workers as subjects of constant experimentation, often in ways that destabilize their economic and even psychological security.[16] In many instances, industries that adopt discourses of technological advancement are driven by precarious worker labor—what Mary Gray and Siddarth Suri describe as *ghost work*.[17]

Such AI systems are correlated with low wages and "flexible" work policies that, in practice, often make it hard for workers to predict their income, schedule, or whether they will even be able to work that day. Similar to other algorithmic management systems, these function by pooling information and power together for the benefit of owners, managers, and a handful of developers, allowing companies to optimize such systems in ways that maximize revenue without regard to the need for stable and livable wages or predictable incomes, schedules, and availability of work. Indeed, many workers have reported being abruptly "kicked off" a gig work platform, and finding themselves unable to work without warning. The process to reinstate an account can be obscure and onerous.[18]

These platforms are continually optimized by companies and owners. Abrupt changes intended to increase revenue for the company can result in significant losses for workers. In one example,

Instacart made changes to its interface that misled customers into thinking they were leaving a tip for workers, when in fact they were paying a service fee to the company.[19] This practice is something that DoorDash also engaged in until July of this year.[20]

These examples demonstrate the significant power asymmetry between workers and customers on one hand, and the companies who control worker management platforms on the other. How, and where, companies may be "optimizing" their platforms at the expense of workers remains largely opaque to anyone outside of companies' corporate offices, and what is known comes largely from worker whistleblowers.

The ability of automated management platforms to manipulate (and arbitrarily cut) wages has been at the heart of worker grievances. Instacart workers report that their earnings decreased precipitously over the last year.[21] Uber and Lyft workers report similar drops.[22] Many identify this as part of a tactic to make workers dependent on the platform for wages, drawing them in with promises of a living wage and flexible working conditions, then severely cutting wages once workers have structured their lives around working for the platform.

Legal scholar Veena Dubal, who has worked with Uber and taxi drivers, makes the case that these practices are not new, but "[reproduce] risky, early 20th century working conditions," enabled by large-scale AI platforms and deregulation.[23] As labor scholar Jim Stanford puts it, "The only thing truly new about gig employment is its use of digital and on-line techniques to assign work, discipline workers . . . and control the money. That's more effective than the bulletin boards and classified ads of yesteryear—but it hardly negates the inherent power imbalance between an individual worker and the multibillion-dollar company they work for."[24]

It is important to note that such concerns do not always translate outside of the US context, which has a history of social security and labor laws whose enforcement has provided some measure of worker protection. This is not the case in many global South regions, where the ability of residents to appeal to the state for resources, along with a history of poorly enforced social safety protections, mean that the role of AI-enabled platform work has a more complex set of implications, which cannot be read through a US-centric lens, and need to account for global histories of colonialism and inequality.[25] For instance, researchers Surie and Koduganti examine platform workers in Bengaluru, India, showing that they exist in a context in which many workers are already stitching together "flexible" work options, without the expectation of social safety nets. Given these existing practices and expectations, AI-enabled platform work provides a comparatively more lucrative source of employment.[26] Similarly, Indian Turk workers (who until recently made up 40 percent of the total platform workforce) benefited from the global pay rates set by the platform, and the cost of living difference between India and the US.[27] This meant that tasks that US workers would not take due to low pay were more attractive for their global South counterparts. In a study of beauty and wellness platforms in India, researchers discovered that women found these platforms attractive because they allowed them to pursue economic activity within the constraints of gendered, religious, and family norms.[28] In these ways, AI-enabled

platform work has challenged the boundedness of local labor markets globally,[29] and brought with it a diverse set of implications that cannot be understood as analogous to the US experience.

AI in Hiring Tech

AI systems to manage and control workers are also being applied in hiring, rapidly and actively shaping the labor market and helping determine who is fit for work, and who isn't. Most hiring tech operates in the absence of any specific rules or requirements to disclose their use for candidate selection, ranking, and hiring to the job seekers whose lives these AI systems affect.[30] Commercial firms across industries, including major employers like Unilever,[31] Goldman Sachs,[32] and Target,[33] are integrating predictive technologies into the process of selecting whom they hire. AI systems also actively shape employment advertising, résumé ranking, and assessment of both active and passive recruitment.[34]

Because AI systems often encode and reproduce patterns of bias within categories such as "competence," "success," and "cultural fit," the rapid deployment of such systems in hiring has significantly raised the stakes of their use.[35] Indeed, many researchers suspect that these tools most likely exacerbate inequity and reinforce discrimination, creating what legal scholar Pauline Kim terms "classification bias."[36] But without meaningful access to these systems and their processes, workers lack the evidence necessary to challenge their use.[37]

Often an early mover on these issues, the state of Illinois has already passed a law pushing back on the secrecy of these systems. So far, it is the only state to do so. Scheduled to take effect in January 2020, the Artificial Intelligence Video Interview Act mandates that employers notify job candidates when artificial intelligence is used in video interviewing, provide an explanation of how the AI system works and what characteristics it uses to evaluate an applicant's fitness for the position, obtain the applicant's consent to be evaluated by AI before the video interview starts, limit access to the videos, and destroy all copies of the video within 30 days of an applicant's request.[38]

Faced with pushback, hiring tech vendors are also attempting to make the case that their systems help fight against historical and human biases, claiming they have been designed to reduce discrimination and increase diversity. Yet at this point, such claims amount to marketing statements and are unsupported by peer-reviewed research. Instead, studies show that there just isn't enough transparency to assess whether and how these models actually work (and to what effect)—let alone to determine whether they're unbiased.[39]

This led the Electronic Privacy Information Center to file a complaint with the Federal Trade Commission alleging that one AI hiring company, HireVue, is engaging in "unfair and deceptive" business practices by failing to ensure the accuracy, reliability, or validity of its algorithmically driven results.[40]

Employers, not workers, are the "customers" whom AI hiring companies seek to court with promises of efficiency and fewer worries about accountability and liability. In fact, several prominent companies, like pymetrics, actively offer to cover any of their customers' legal fees or liabilities that might arise from the use of their products or services.[41]

AI-driven hiring systems are only the starting point of a concentrated push to use AI to monitor and control workers and workplaces—as Ifeoma Ajunwa and Daniel Greene put it, these platforms "create a managerial framework for workers as fungible human capital, available on demand and easily ported between job tasks and organizations."[42]

It's critical that researchers and advocates not only examine the application of artificial intelligence in the hiring process in isolation, but also consider how AI is being implicated in broader shifts in labor practices, and how it might be serving to define and redefine notions of competence and ability.[43]

Labor Automation's Disparate Impacts

In recent years, two predominant narratives have emerged around the future of work and labor automation.[44] One insists that labor automation will yield a net gain for society—increasing productivity, growing the economy, and creating more jobs and demand for workers that will offset any technological displacement that happens along the way.[45] The other predicts a labor apocalypse, where robots will ultimately take over the workforce, create massive unemployment, and serve only the financial interests of those who own them and the engines of our economy.[46] Both narratives are predicated on the assumption that automation in the workplace is inevitable and that automated systems are capable of performing tasks that had previously been the work of humans.

What is missing from both conflicting narratives is the more nuanced prediction of who will be harmed and who will benefit from labor automation in the years to come. This year, more data emerged that begins to provide the following answer to those questions: labor automation and the corresponding restructuring and reduction in waged work will likely disproportionately harm Black, Latinx, and low-wage workers in the US.

One such study from the Brookings Institute predicts that certain demographic groups will likely bear more of the burden of adjusting to labor automation than others, implying that the benefits of automation—increased efficiency and profit—are not shared with all workers, but accrue to those at the top.[47]

First, the study found that lower-wage workers stand to lose the most due to automation while white-collar workers will likely remain largely unaffected. Using a model that views a job as a bundle of tasks (some of which can be automated and others not), Brookings concluded that the average "automation potential" for US occupations requiring less than a bachelor's degree is 55

percent—more than double the 24 percent susceptibility among occupations requiring a bachelor's degree or more.[48] That means US workers in occupations that pay the least, like food preparation and serving, production jobs in factories, and administrative support—which pay wages of only 50 to 75 percent of the national average—could experience 60 to 80 percent task-level disruption.[49] Meanwhile, higher-paying jobs in business and financial operations or engineering, where US workers earn 150 percent of the average wage, will likely experience as little as 14 percent of their current tasks being displaced by automation.

This has serious implications in terms of the risk exposure faced by certain communities. Black, Native American, and Latinx workers who make up a larger proportion of the workforce in occupations like construction, agriculture, and transportation[50] face average task-automation potentials of 44 to 47 percent. That's anywhere from five to eight percent more than their White counterparts.[51]

The disparate effects of task automation will also likely entail disproportionate job losses. Even McKinsey & Company, which believes AI could lift productivity and economic growth, concluded that labor automation will further exacerbate the racial wealth gap in the US absent any interventions.[52] One study from July 2019 found that more than a quarter of Latinx workers—as many as seven million people—are in jobs that could be automated by 2030.[53] That translates to a potential displacement rate of 25.5 percent for Latinx workers, three percentage points higher than the national average.[54] McKinsey calculated that 4.6 million Black workers will be displaced by 2030 due to automation, with a potential displacement rate of 23.1 percent.[55]

The exact job-loss figures caused by automation are ultimately hotly contested. After *MIT Technology Review* synthesized 18 different reports on the effects of automation on labor with predictions ranging from a gain of nearly 1 billion jobs globally by 2030 to a loss of 2 billion, it aptly noted that "prognostications are all over the map."[56] With all of these projections, the devil is in the details. We may "have no idea how many jobs will actually be lost to the march of technological progress,"[57] but we can begin to answer *who* will lose their jobs based on the power dynamics and economic disparities that already exist today.

The Limits of Corporate AI Ethics

This year, many companies, governments, NGOs, and academic institutions followed the familiar path of generating AI ethics principles and statements. These primarily Western entities—many of them driven by an industry that is predominantly White, male, and wealthy—often present such ethics principles as the product of a growing "global consensus" on AI ethics. This promotes a majoritarian view of ethics, which is especially concerning given the widespread evidence showing that AI bias and misuse harms the very people whose voices are largely missing in ethics debates.[58]

There are now so many ethics policy statements that some groups began to aggregate them into standalone AI ethics surveys, which attempted to summarize and consolidate a representative sample of AI principle statements in order to identify themes and make normative assertions about the state of AI ethics.[59] Despite the increase in AI ethics content and corresponding meta-analyses, ethical principles and statements rarely focus on how AI ethics can be implemented and whether they're effective. Similarly, such AI ethics statements largely ignore questions of how, where, and by whom such guidelines may be operationalized.

These surveys tend to aggregate AI ethics content from a very wide variety of contexts, blending corporate statements released on corporate blogs,[60] publicly informed governing declarations,[61] government policy guidelines from national and coalition strategies,[62] and nonprofit mission statements and charters.[63] However, they usually lack a comprehensive account of the methods used and sometimes equate internal and often secret corporate decision-making processes with grassroots-driven statements and governmental policy recommendations.

The vast majority of these documents were generated from countries and organizations in the global North.[64] Principle statements and the ethical priorities of the global South with regard to artificial intelligence are often absent from these surveys.

Scholars and advocates have increasingly called attention to the gap between high-level statements and meaningful accountability.[65] Critics have identified conflicting ideals and vague definitions as barriers that are preventing the operationalization of ethics principles in AI product development, deployment, and auditing frameworks. In "Principles Alone Cannot Guarantee Ethical AI," philosopher and ethicist Brent Mittelstadt makes the observation that, unlike medicine, AI has no formal professional governance structure or norms—no agreed-upon definitions and goals for the field.[66] Most importantly, unlike medical ethics, AI ethics has no external oversight or standard protocols for enforcing ethical guardrails.

This lack of professional and legal accountability undermines corporate ethics approaches. One example is Microsoft's funding of an Israeli facial-recognition surveillance company called AnyVision that targets Palestinians in the West Bank.[67] AnyVision facilitates surveillance, allowing Israeli authorities to identify Palenstenian individuals and track their movements in public space. Given the documented human-rights abuses happening on the West Bank,[68] together with the civil-liberties implications associated with facial recognition in policing contexts,[69] at a minimum, this use case directly contradicts Microsoft's declared principles of "lawful surveillance" and "non-discrimination," along with the company's promise not to "deploy facial recognition technology in scenarios that we believe will put freedoms at risk."[70] More perplexing still is that AnyVision confirmed to reporters that their technology had been vetted against Microsoft's ethical commitments. After public outcry, Microsoft acknowledged that there could be a problem, and hired former Attorney General Eric Holder to investigate the alignment between AnyVision's actions and Microsoft's ethical principles.[71]

In another of many such examples of corporations openly defying their own ethics principles, and despite declaring as one of its AI principles to "avoid creating or reinforcing unfair bias,"[72] Google set up the Advanced Technology External Advisory Council (ATEAC), an ethics board that included Kay Coles James, the president of the Heritage Foundation and someone known for her transphobic and anti-immigrant views. Workers and the public objected. A petition signed by over 2,500 Google workers argued: "In selecting James, Google is making clear that its version of 'ethics' values proximity to power over the wellbeing of trans people, other LGBTQ people, and immigrants. . . . Not only are James' views counter to Google's stated values, but they are directly counter to the project of ensuring that the development and application of AI prioritizes justice over profit."[73] Following the backlash, Google dissolved ATEAC after a little over a week.[74]

Yet even if one believes that corporate AI ethics might help guide better tech practices on some level, it is clear that change in the design, development, and implementation of AI systems largely occurs when there is pressure on companies from workers, the press, and policymakers. For example, the various controversies Facebook has publicly faced demonstrate that public pressure and organized workers appear to be far better at ensuring ethical AI than principles. Facebook advertises its own internal ethics process. However, investigative reports from outlets such as ProPublica on Facebook's discriminatory online advertising filtering mechanisms together with published studies about Facebook's online ad ecosystem bolstered lawsuits brought by the Department of Urban Housing and Defense, civil rights groups, and labor organizations against the company in 2019.[75]

Given the concerns that ethical promises are inadequate in the face of urgent accountability gaps, many have argued that human rights principles, which are based on more established legal interpretations and practice, should replace "ethics" as the dominant framework for conversations about AI governance and oversight. Advocates for this approach describe human rights as ethics "with teeth," or an alternative to the challenge of operationalizing ethics.[76]

The human rights legal framework has its own potential shortcomings, especially as it relates to AI technology.[77] One of these limitations is the challenges of enforcement of international human rights law when it pertains to powerful nations. Given that the US and China are considered global AI leaders that have both engaged in varying degrees of documented human rights abuses without facing meaningful consequences under international human rights law,[78] expecting human rights frameworks to constrain governmental and corporate actors within the countries currently dominating AI development may be impractical. Indeed, human rights law is mainly focused on government actors, so beyond the current lack of enforcement, the question of how it might serve to curb corporate malfeasance remains unanswered.

By claiming a commitment to ethics, companies implicitly claim the right to decide what it means to "responsibly" deploy these technologies, and thus the right to decide what "ethical AI" means for the rest of the world.[79] As technology companies rarely suffer meaningful consequences when their ethical principles are violated, true accountability will depend on workers, journalists,

researchers, policymakers, and the public continuing to be at the forefront of the fight against the harmful uses of this technology.

Some advocates are also pushing to ensure that engineers and developers are trained in ethics, and thus, the thinking goes, better capable of making more ethical decisions that can ensure more ethical tech. Barbara Grosz, a professor of natural sciences, imagines a world in which "every time a computer scientist logs on to write an algorithm or build a system, a message will flash across the screen that asks, 'Have you thought about the ethical implications of what you're doing?'"[80] The Design Justice Network takes this further, centering justice, not ethics, and calling on developers and designers to center affected communities in the process of creating technology together.[81]

AI developers and researchers make important determinations that can affect billions of people, and helping them consider whom the technology benefits and harms is important. The case of Uber's self-driving car makes clear what could have been had engineers, designers, and executives put more care into ethics and safety (although whether or not these were decisions engineers had the power to make is not something we know). In 2018, an autonomous Uber in Arizona killed Elaine Herzberg, a pedestrian. A recent National Transportation Safety Board investigation found significant problems with Uber's autonomous system, including a shocking disclosure that Uber's self-driving software "wasn't designed to expect that pedestrians outside crosswalks may be crossing the street."[82] Similar engineering failures led to over 37 accidents involving autonomous Uber vehicles.[83] It is clear that better testing and engineering practices, grounded in concern for the implications of AI, are urgently needed.

However, focusing on engineers without accounting for the broader political economy within which AI is produced and deployed runs the risk of placing responsibility on individual actors within a much larger system, erasing very real power asymmetries. Those at the top of corporate hierarchies have much more power to set direction and shape ethical decision-making than do individual researchers and developers. Such an emphasis on "ethical education" recalls the push for "unconscious bias" training as a way to "improve diversity." Racism and misogyny are treated as "invisible" symptoms latent in individuals, not as structural problems that manifest in material inequities. These formulations ignore the fact that engineers are often not at the center of the decisions that lead to harm, and may not even know about them. For example, some engineers working on Google's Project Maven weren't aware that they were building a military drone surveillance system.[84] Indeed, such obscurity is often by design, with sensitive projects being split into sections, making it impossible for any one developer or team to understand the ultimate shape of what they are building, and where it might be applied.[85]

How AI Companies Are Inciting Geographic Displacement

Just as the development environments of artificial intelligence and machine learning are filled with disparities, so too are the broader cityscapes in which their development takes place. Whether within large suburban tech campuses or smaller urban tech start-ups, AI and machine learning environments are never contained within company walls. Rather, the racial, gendered, and class-based biases well proven to exist within AI labs are porous, spilling into external spaces. Often this results in processes popularly described as tech-driven gentrification, or the replacement of poor, working-class, and/or racialized residents with wealthier and whiter tech employees.

While numerous cities have experienced AI displacement, San Francisco has been especially impacted. With the IPO releases of a number of tech companies this past year, the real estate industry has predicted a new surge of tech wealth. As during the dot-com boom, speculators disproportionately evict Black and Latinx working-class tenants in order to create new housing for wealthier and whiter tech employees.[86]

Meanwhile, across the Bay, Alameda and Contra Costa counties, which were devastated by the 2008 foreclosure crisis, continue to see the loss of Black and Latinx homeownership and housing. In fact, the subprime crisis and the fintech derivatives market it relied upon can also be understood as a technology of AI displacement.[87] The very algorithms used by lenders and banks relied upon codifying Black homeowners as exploitable.[88] In the post-2008 era, Wall Street investment firms such as Blackstone/Invitation Homes use machine learning systems to calculate rental acquisitions, buying up huge swaths of property foreclosed during the subprime crisis and renting them out as single-family homes.[89] They rent such homes out today using proptech AI management systems and property databases known to engage in tenant profiling that disfavors people of color.[90]

This era has also been marked by the 2008 launch of Airbnb, the San Francisco start-up linked to ongoing gentrification of cities worldwide as long-term tenants are replaced with tourists.[91] Even single room occupancy hotels (SROs), which have historically housed precarious residents, have been converted into “tech dorms” and tourist accommodations in cities such as San Francisco and Oakland.[92]

Also characteristic are the private tech luxury buses that facilitate reverse commuting of tech workers to Silicon Valley from urban centers. Landlords have found property adjacent to “Google bus stops” lucrative, leading to increased rental prices and evictions along with new luxury and market-rate development projects.[93] [94]

While eviction trends often appear bleak, gentrification has not transpired without resistance. As during the dot-com boom and foreclosure crisis, numerous organizations and collectives formed to organize for housing justice. Existing housing organizations also rose to the occasion, and new

efforts, such as the Anti-Displacement Coalition in San Francisco and the Bay Area-wide Tenant Organizing Network, were formed. Rent-control protection groups and tenant unions have been forming monthly, and statewide tenant organizing has been on the rise.[95] AI displacement is not limited to San Francisco, or even to the United States, where most major AI companies reside. For instance, Cluj, Romania, the supposed "Silicon Valley of Eastern Europe," has become one of many AI and IT outsourcing locales.[96] The laborers there often make more than their neighbors. Increasingly, they are able to rent and buy fancier flats adjacent to outsourcing offices, which has incentivized the city to evict racialized Roma residents. Accordingly, housing justice groups such as Social Housing Now (Căsi Sociala Acum) are in the midst of organizing against evictions and for the development of social housing.[97]

Back in the North, there have been new forms of international solidarity in the works against AI displacement. For instance, current organizing against Google's proposed new campus in San Jose is being led by groups such as Serve the People San Jose. As they have argued, Google's new campus will lead to mass displacement and unaffordability. Thus they have been organizing marches, Google bus blockades, and City Council demonstrations.[98] Much of this has taken place in solidarity with organizers and groups in Berlin such as Google Is Not a Good Neighbor (Google ist kein guter Nachbar), which in 2018 collectively blocked Google from launching a new tech campus in the neighborhood of Kreuzberg.[99] Solidarity has also been found among New York City organizers who successfully fought the development of a new Amazon campus in 2019, and with activists in Toronto committed to thwarting gentrification induced by Sidewalk Labs.[100]

During demonstrations, banners, light projections, video clips, and statements of support have expressed international solidarity, revealing a new trend toward urban justice.[101] Much work remains to link struggles against forms of tech-sector displacement worldwide.

1.2 Organizing Against and Resisting Consolidations of Power

Organizing and Pushback

Pushback against AI isn't new, nor is it confined to tech companies and elite universities. Often, it's not even identified as related to biased and harmful AI. This is in part because AI systems are often integrated "in the backend," as part of operationalizing larger policies which themselves are the focus of organizing. Because AI technologies are often applied in ways that amplify and exacerbate historical patterns of inequality and discrimination, it is these historical practices—not AI systems alone—to which organizers and communities seeking justice are reacting.

Community Organizing

Community organizers have been an important force in the pushback against harmful AI. This was most visible in the wave of community organizing this year tackling the use of facial recognition in cities around the world: San Francisco,[102] Oakland,[103] Somerville,[104] Montreal,[105] and Detroit,[106] among others. Community-driven organizing led directly to bans on facial recognition in many of these localities. As we highlight elsewhere in this report, in Brooklyn, tenants of Atlantic Plaza Towers organized and successfully challenged the incorporation of a facial recognition system into their building.[107]

Community organizers also played a critical role in mapping the connections between mass incarceration, the surveillance of communities of color, and the push to adopt predictive policing tools. In Los Angeles, community organizers successfully advocated for a temporary suspension of the Los Angeles Police Department's use of the predictive policing program LASER, which purported to identify individuals likely to predict violent crimes. The Stop LAPD Spying Coalition[108] argued that the department used proxy data to discriminate against Latinx and Black community members.[109] In this effort, they were joined by UCLA students who signed a public-facing letter denouncing UCLA research and development of the predictive policing tool PredPol. Citing evidence of the role of such tools in perpetuating the overpolicing of communities of color, they requested UCLA researchers abstain from further development and commercialization of the tool.[110] Here we see students and communities acting to operationalize a critique of predictive policing that some AI researchers have made in recent years.[111] We discuss the growing student movement against harmful tech and exclusionary tech cultures in more detail below.

In St. Louis, Missouri, residents also demonstrated against policing tech, protesting a proposed agreement between St. Louis police and a company called Predictive Surveillance Systems to deploy surveillance planes to collect images of citizens on the ground. They asserted that the "suspicionless tracking" would be an invasion of citizens' privacy.[112]

In Kansas, New York, Pennsylvania, and Connecticut, parents opposed the use of a web-based educational platform called Summit Learning in their schools. High schoolers staged sit-ins, and parents protested at school board meetings, emphasizing that the work of teachers could not be outsourced to technology-based platforms. And in Pennsylvania and Connecticut, they were successful in getting the Summit programs cut.[113]

The community group Mijente, which describes itself as a political home for multiracial Latinx and Chicanx people, has been at the forefront of mapping the connections between AI and immigration, and building broad coalitions. In July, Mijente joined Media Justice (an organization at the helm of San Francisco's facial-recognition ban)[114] and Tech Workers Coalition[115] to host Take Back Tech. The event convened community organizers alongside tech workers and

students, aiming to share strategies and knowledge, and to build coalitions between those harmed by oppressive technologies and those close to the research and development of such tech.[116]

In August of this year, Mijente released a detailed report based on FOIA record requests illuminating the central role certain technologies have played in detaining Black and Brown people, and the use of these technologies in immigration enforcement.[117] The organization also spearheaded the #NoTechforICE campaign in opposition to the Trump Administration's raids and mass deportations of migrants along the southern border of the US. This work helped shed light on lucrative tech company contracts with military and border agencies, and mobilized tech workers and students, while also emphasizing the human cost of a deportation campaign rife with human rights abuses.[118] Protesters catalyzed by the campaign have held regular demonstrations at Palantir's headquarters in Palo Alto and at its New York City offices.[119]

Organizations such as Never Again Action,[120] and Jews for Racial and Economic Justice (JFREJ)[121] have also led highly visible actions against Amazon, organizing street protests and sit-ins in Amazon bookstores to protest against the company's ongoing work providing cloud computing services to ICE.[122] And Immigrant rights groups such as Make the Road New York,[123] along with Mijente, JFREJ, and other advocates, have reached out to academics and computer science and technology professionals through petitions, demanding that prominent conferences drop Palantir as a sponsor, given the company's role in empowering ICE.[124] Community-organized opposition to Palantir's role in ICE's detention of immigrants resulted in UC Berkeley's Privacy Law Scholars Conference,[125] Lesbians Who Tech,[126] and the Grace Hopper Celebration all pulling Palantir as a sponsor.[127]

Athena, a recently launched coalition, takes this further. Targeting Amazon, the coalition includes groups like ALIGN, New York Communities for Change, Make The Road New York, Desis Rising Up and Moving, and many others who successfully campaigned to challenge Amazon's plans to build its HQ2 in Queens, New York.[128] The campaign against Amazon's HQ2 was notable for its broad multi-issue approach, and for its somewhat unexpected success. Advocates and community organizers criticized the company's tax avoidance, the displacement that would follow in the wake of such a massive tech company headquarters, and the lavish corporate subsidies that New York offered the company. But they also organized around issues like Amazon's treatment of warehouse workers and its sale of surveillance tech.[129] Athena expands on this multi-issue approach, recognizing that Amazon is at the heart of a set of interlocking issues, including worker rights at warehouses, climate justice, and mass surveillance. The coalition includes organizations with experience across these domains, and is working to unify the growing opposition to the company and develop strategies capable of tackling AI companies whose reach extends into so many sensitive domains.[130]

These are only a handful of instances where community organizers are pushing back against AI and oppressive tech. Collectively, they highlight that the pushback against AI is not necessarily just about AI, but about policies and practices that exacerbate inequality and cause harm to our

communities. They also demonstrate that AI does not exist in isolation—it builds upon historical surveillance and policing practices that predominantly impact Black communities, communities of color, and the poor.[131]

Acknowledging and making these processes visible is an important step toward decentering technology in this conversation. A focus on AI systems can obscure and abstract what are fundamentally *institutional* decisions masked by a technical veneer that excludes the communities most affected from having a voice in the process. The pushback against AI thus builds upon the social justice work that organizers have engaged in for a much longer time. Researchers can play an important role in this conversation by demystifying AI systems, pushing back on discourses that privilege technology, and listening closely to the communities leading these efforts.[132]

Worker Organizing

Although organizing among tech workers has been underway for many years (spurred initially by contract workers), worker organizing around the harms of AI is relatively new. Such organizing is situated within a broader effort to address overall worker issues, ranging from wages and working conditions to concerns about respect, diversity, and inclusion, that seek to directly confront hostile workplace cultures. This broad organizing platform has resulted not only from coordinated efforts between cross-sector worker groups but also from the increased realization that workers and communities generally considered separate or distinct share common concerns when it comes to AI and large-scale technical systems.

For example, tech workers have joined with community organizers in pushing back against tech's role in perpetuating human rights abuses and maltreatment of migrants and Latinx residents at the southern US border. Since the fall of 2018, workers at Salesforce,[133] Microsoft,[134] Accenture,[135] Google, [136] Tableau,[137] and GitHub[138] all signed petitions and open letters protesting their companies' contracts with ICE. Developer Seth Vago pulled his open-source code out of the codebase used by the company Chef after learning of the company's contract with ICE.[139] This led Chef to commit to cancel their contract, and spurred a larger discussion about the ethical responsibility of developers.

Even workers at Palantir, the tech company at the center of ICE's detention and tracking operations, circulated two open letters, and have expressed mistrust of and frustration with the company's leadership for its decision to keep its contract with ICE.[140] Palantir CEO Alex Karp has publicly defended this work,[141] and in August the company renewed a contract worth $49 million over three years.[142]

Other workers protested the development of military AI systems: Microsoft employees signed an open letter to the company asking it not to bid on JEDI, a major Department of Defense cloud-computing contract, which the company ultimately won.[143] In February, employees at the

company followed this with a call to cancel a $480 million contract to provide augmented reality headsets to the US military, saying they did "not want to become war profiteers."[144]

Such examples demonstrate how tech workers' strategies build solidarity with the communities most affected by AI's harmful uses. Worker organizing around AI is also part of a broader tech-worker movement focused on a broad range of social justice issues, including displacement,[145] two-tiered workforces and the exploitation of contract workers,[146] and climate change. In April, 8,695 Amazon workers publicly signed a letter calling on the company to address its contributions to climate change through a shareholder resolution,[147] and staged a walkout in September in the face of inaction by the company.[148] The September climate walkout was the first labor action coordinated across multiple tech companies, and provides an indication of the growth of tech-worker organizing during 2019.

While the Google Walkout was, so far, the largest global labor action in tech,[149] it was only the first of many. Employees at Riot Games walked out in protest of the company's stance on forced arbitration, following allegations by multiple employees that the company violated California's Equal Pay Act and claims of gender-based discrimination and harassment.[150] In China, developers protested what they described as the 996 schedule—9 a.m. to 9 p.m., six days a week—through a GitHub repository of companies and projects asking for excessive hours.[151] And in November, Google workers again walked out, hosting a rally of hundreds of workers in San Francisco protesting retaliation against two organizers.[152] Following this rally, Google fired four organizers, signaling both the growing power of such efforts to impact Google and the company's intolerance of them.[153]

Another key development was contract workers leading the recent wave of tech-worker organizing,[154] centering the risks they experience as a result of the two-tier labor systems in which they work. In particular, contract workers lack the benefits, stability, and pay of their employee colleagues, a disparity often enacted along racial lines. A 2016 report from Working Partnerships USA found that 58 percent of blue-collar contract workers in tech are Black and Latinx, and make an average of $19,900 annually. The report found that only 10 percent of "employee" tech workers are Black or Latinx, and that these workers make over $100 thousand annually.[155] Tech workers have called for an end to such discrimination, noting the racial divide and its implications for the perpetuation of structural inequality.[156]

In spite of the precarity and disadvantages that come with being classified as a contract worker, these workers continued to organize, from temp workers at Foxconn factories protesting unpaid wages and bonuses promised to them by recruitment agencies[157] to workers at Amazon warehouses walking out on Prime Day and successfully winning compromises to improve conditions.[158] Beyond protesting workplace conditions, contract workers have been leaders in pushing for ethical company practices, with Amazon-owned Whole Foods workers publishing a letter demanding Amazon end its involvement with ICE[159] and sharing a video revealing the company's union-busting tactics.[160]

Such organizing has led to a wave of unions forming among workers on the corporate campuses of tech firms in recent years, a trend that started in 2014, well before white-collar workers began visibly organizing. These included food-service workers at Airbnb,[161] Facebook,[162] and Yahoo,[163] and shuttle drivers and security guards at a host of Silicon Valley firms.[164] In Poland, Spain, and Germany, unionized Amazon warehouse workers held strikes to demand higher pay and better working conditions.[165]

But Amazon and other tech companies are using tactics to prevent unions from forming: for example, 14 software engineers at the start-up Lanetix were fired shortly after unionizing earlier this year. The workers filed charges with the National Labor Relations Board and ultimately won their case.[166] Google also hired a consulting firm known for its anti-union work amid employee unrest, a fact disclosed by whistleblowers.[167]

Globally, strikes by transport workers grew in response to ride-sharing apps that are decreasing wages and living standards. Uber drivers staged major strikes in cities around the globe[168][169][170] including drivers' occupying Uber's offices in France,[171] while Ola drivers in India protested decreasing driver incentives amid increasing fuel prices.[172] China Labor Bulletin recorded nearly 1,400 transport worker protests over a five-year period in cities across the country.[173]

In the state of California, driver protests resulted in significant and tangible gains—though not from the companies themselves. Instead, California's State Assembly passed Assembly Bill 5 (AB5), which makes it much harder for companies like Uber to label workers as independent contractors, granting them basic worker protections.[174] In arguing against the change, Uber claimed that drivers weren't core to Uber's business, and thus the company should not have to reclassify them as employees.[175] Based on this argument, Uber and Lyft appear likely to take their case to court.[176][177] AB-5 in California was followed swiftly by a ruling in New Jersey that argued Uber had misclassified drivers as independent contractors, and demanded the company pay $649 million in unpaid employment taxes.[178]

At the close of 2019, the pushback against the two-tier labor system appears poised to expand more widely: responding to worker protests, a group of US senators wrote Google CEO Sundar Pichai expressing objection to the company's heavy reliance on temporary workers (over half its workforce)[179] and urging the company to end its abuse of worker classifications.[180] Such reclassification of workers would result in thousands of people gaining access to essential benefits, workplace protections, and stability, which are denied contract workers. A move to reclassify all workers as employees would also have significant implications for the production and maintenance of AI systems, since low-paid contract workers are an essential labor force labeling AI training data, and moderating content on large algorithmically driven platforms.

Student Organizing

In organizing against contracts with ICE and military AI, community organizers and workers were joined by students. Engineering students in particular have significant leverage, given that tech companies compete to recruit top talent and view them as "future workers."[181] Ethically minded students are having an impact on recruiting. Facebook already has seen its offer acceptance rate dwindle from 85 percent to 35–55 percent at top computer science schools, as students begin to look beyond compensation and reflect on the commitment to ethics, diversity, and accountability demonstrated by the companies they hope to join.[182]

In the fall of 2018, students at Stanford first circulated a pledge not to accept interviews from Google until the company canceled its work on Project Maven, a US military effort to build AI-enabled drone surveillance, and committed to no further military involvement.[183] This movement grew significantly during 2019, spearheaded by Mijente's #NoTechForICE campaign. Students around the US demonstrated against recruiting events on campus by technology companies known to be supporting border control or policing activities, such as Amazon, Salesforce, and Palantir.[184] Over 1,200 students representing 17 campuses signed a pledge asserting they would not work at Palantir because of its ties to ICE.[185]

In February, students from Central Michigan University fought against the creation of a university Army AI Task Force that was poised to endorse the military use of AI.[186]

Today's growing student movement targeting tech and military recruitment recalls historic student demonstrations against recruiting efforts, such as those by the CIA. In the 1960s, Brown University and Stanford University students disrupted CIA on-campus interviews in opposition to their involvement in Vietnam[187]. Similarly, University of Connecticut students in the early 1970s refused to accept the inclusion of Dow Chemical and Olin Mathieson in their on-campus events, as the chemical engineering companies contributed to chemical defoliants used in the Vietnam War. This movement later grew into an all-out campaign demanding the university's divestment from the military-industrial complex, and affiliated organizations such as the on-campus Reserve Officers Training Corps (ROTC).[188]

Student organizing also focused on racist, misogynist, and inequitable cultures within universities, tying these to unethical funding practices, and close relationships to military and surveillance interests. At MIT, graduate student Arwa Mboya was one of the first to call for accountability after revelations surfaced showing the MIT Media Lab's close funding relationship with child sex trafficker and assailant Jeffery Epstein.[189] Mboya called on Media Lab Director Joi Ito to resign from his position. After investigative journalist Ronan Farrow reported on the ties between Epstein and Ito's Media Lab, Ito stepped down.[190] Responding to these disclosures, groups like MIT Students Against War organized protests and town halls, demanding that MIT President L. Rafael Reif and "all senior leadership that was aware of this issue" resign. They also demanded a board

made up of students, faculty, and staff to review and approve donations.[191] In doing so, they made the case that the Epstein revelations were one of many examples of MIT's misogynistic culture, pointing to the university's continued employment of undergraduate professor Seth Lloyd, who visited Jeffery Epstein in prison and continues to defend the relationship.[192]

The diverse concerns animating student organizing, and the way in which organizers are tracing the interconnections between them, echoes the breadth of focus of the tech-worker movement, and a growing recognition that hostile tech cultures are reflected in the technology produced within such cultures.

1.3 Law and Policy Responses

This year, interest in regulating AI systems increased, with a focus on data protection, algorithmic accountability, and biometric/facial-recognition safeguards. Building on the emergence of globally oriented data protection approaches such as the European Union's General Data Protection Regulation (GDPR), policymakers are moving quickly, driven both by the current sense of urgency to regulate the mass deployment of AI technologies lacking discernible safeguards and by the failure of ethical frameworks to adequately answer the call for accountability and justice.

Data Protection as the Foundation of the Majority of AI Regulatory Frameworks

The relative success of data-protection laws to confront and contain harmful behaviors by technology companies provides a natural foundation for approaches to new forms of algorithmic activity.[193] In particular, the right to access one's personal data,[194] to access information about automated decision-making,[195] and requirements like data protection impact assessments (DPIAs) and privacy by design align well with most AI accountability frameworks.[196] As legal scholars Margot E. Kaminski and Gianclaudio Malgieri argue, DPIAs are a bridge between "the two faces of the GDPR's approach to algorithmic accountability: individual rights and systemic collaborative governance."[197]

As governments now move to regulate algorithmic systems, they are not doing so in a policy vacuum. More than 130 countries[198] have now passed comprehensive data protection laws, with Kenya[199] and Brazil[200] being the latest to have modeled their laws largely on the GDPR. While the US still lacks a general data protection law, momentum appears to be growing to address this gap, with a dramatic increase in activity at both the federal and state levels.[201]

However, there is still an ongoing debate about whether GDPR-style frameworks can or should offer a "right to explanation" about specific automated decisions. Some scholars argue that no such right presently exists in the GDPR,[202] while others argue that multiple provisions of the GDPR

can be pieced together to obtain meaningful information about the logic involved in automated decisions.[203] It remains to be seen if this is an effective or even available tool for accountability, as there continues to be a debate over the ways in which transparency[204] and other ways of "seeing through data protection laws" can engage with the goals of algorithmic accountability frameworks.

Biometric Recognition Regulation

This year, numerous regulatory attempts emerged to address the privacy, discrimination, and surveillance concerns associated with biometrics—the measurement of unique biological characteristics, including data used in facial and affect recognition. These regulatory attempts range from bans or moratoriums to laws that would allow the technology on a case-by-case basis with specific forms of oversight.

In Europe, the Swedish government fined a high school for its facial-recognition attendance registry as a violation of GDPR.[205] France's data protection authority, CNIL, declared it illegal to use facial recognition in schools based on privacy concerns.[206]

The Australian Parliament took a more aggressive approach, ordering a complete pause on the use of a national face database. The moratorium will not be lifted until legislation emerges that will allow the government to manage and build the system while acknowledging citizen digital rights and develop a proposal that prioritizes "privacy, transparency and . . . robust safeguards."[207] American cities such as San Francisco, Oakland, Seattle, and Somerville similarly have voted to ban all forms of government use of the technology.[208]

In 2019, members of the United States Congress proposed several biometric bills, including the Commercial Facial Recognition Privacy Act of 2019,[209] the Facial Recognition Technology Warrant Act,[210] and the No Biometric Barriers Act of 2019.[211] The latter seeks to prohibit biometric recognition in public housing, highlighting many of the same concerns as the tenant organizing at Atlantic Plaza Towers in Brownsville, Brooklyn, where residents sought to keep their landlord from installing an invasive facial-recognition system in their rent-stabilized apartment complex.[212]

Biometric recognition also emerged this year as a pressing campaign issue. Notably, Democratic presidential nominee candidates have publicly taken various stances on the topic, with Senator Bernie Sanders adopting the strongest position of calling for a total ban of police use of the technology.[213]

Meanwhile, several states in the US—Washington,[214] Texas,[215] California,[216] Arkansas,[217] New York,[218] and Illinois[219]—have begun actively restricting and regulating in these areas, including limits on some forms of biometric collection and recognition. In addition, Washington,[220] Michigan,[221] California,[222] Massachusetts,[223] Arizona,[224] and Florida[225] have introduced efforts seeking to do the same.

Several proposals, such as the Florida Biometric Privacy Act, the California Consumer Privacy Act, Bill S. 1385 in Massachusetts, NY SB 1203 in New York, and HB1493 in Washington, are explicitly modeled after Biometric Information Privacy Act (BIPA), a 2008 Illinois privacy act that serves as a high watermark. This is especially true after the Ninth Circuit Court of Appeals approved the pursuit of an Illinois class-action lawsuit under BIPA against Facebook's use of facial-recognition technology in August, finding that Facebook's collection of biometric face data from users injured their rights to privacy.[226]

Key corporate developers of the technology—including Microsoft[227] and Amazon[228]—have also come out in support of various forms of regulation on use but have generally resisted[229] calls for bans or moratoriums. This strategy mirrors the historic approaches tech companies have taken to data protection and other regulatory frameworks that emphasize production pathways and compliance over regulatory approach, oversight, and intervention.

Internal corporate conversations have also addressed regulation. Amazon attempted to block a shareholder vote on pausing the company's sale of facial-recognition technology until a third-party confirmation that "it does not cause or contribute to actual or potential violations of human rights." Even after the vote was allowed to go forward by the Securities and Exchange Commission (SEC),[230] Amazon aggressively campaigned for shareholders to vote against the ban.[231] Body camera manufacturer Axon,[232] in contrast, has adopted an internal ban policy. It remains to be seen what concrete impact these efforts will have.

As the biometric-recognition industry moves full speed ahead with massive investments in production and deployment, governments are adopting the technology at a faster rate than they are regulating it. France has announced plans to establish a national facial-recognition database.[233] In the UK, police in Cardiff and London both began trial use of facial-recognition technology, leading to legal challenges and objections by civil society groups, academics, and at least one department's ethics committee.[234] This year, news of China's use of biometric recognition as weapons of state power to target a Muslim minority[235] and Hong Kong protestors[236] made international headlines. In Hong Kong, such surveillance violated their own GDPR-style Personal Data (Privacy) Ordinance (PDPO),[237] but China declared a state of emergency and overrode it.

Algorithmic Accountability and Impact Assessments

This year, algorithmic accountability bills profilerated, especially in the United States. As noted above, US lawmakers introduced the AAA, which would authorize the Federal Trade Commission (FTC) to assess whether corporate automated decision systems (ADS) products are biased, discriminatory, or pose a privacy risk to consumers. It also requires ADS vendors to submit impact assessments to the FTC for evaluation.

As AI Now's 2018 report highlighted,[238] the use of algorithmic impact assessments (AIAs) has been gaining traction in both policy circles and various countries, states, and cities.[239] Built on the success of data-protection, environmental, human-rights, and privacy-impact assessments, AIAs require AI vendors and their customers to understand and assess the social implications of their technologies *before* they are used to impact people's lives. As we outline in our AIA framework,[240] these assessments would be made publicly available for comment by interested individuals and communities as well as researchers, policymakers, and advocates to ensure they are safe for deployment and that those who make and use them are acting responsibly.

For example, Canada's implementation of AIAs appears under its Directive on Automated Decision-Making, as part of the Pan-Canadian AI Strategy,[241] where the Department of Treasury embeds the tool into their government procurement process. Australia's AI Ethics Framework also contemplates the use of AIAs.[242] Washington became the first state to propose AIAs for government ADS with its House and Senate bills HB 165[243] and SB 5527.[244] In addition, some scholars have also advocated for a model AIA to complement DPIAs under the GDPR.[245]

Another dimension to this year's algorithmic accountability legislation was algorithmic transparency. As law enforcement agencies increasingly turn to proprietary technology in criminal proceedings, the intellectual-property rights of private companies are being pitted against defendants' right to access information about that technology in order to challenge it in court. Addressing the specific case of forensic algorithms like automated software used to analyze DNA and predict potential suspects, the Justice in Forensic Algorithms Act of 2019[246] prohibits companies from withholding information about their system, such as its source code, from a defendant in a criminal proceeding on trade-secrecy grounds.

Experimentation with Task Forces

Technologies like predictive analytics and ADS present a number of risks and concerns, especially when used by government agencies to make sensitive determinations around who receives benefits, which school a child attends, and who is released from jail. Recognizing these risks, governments at all levels have begun working to address these concerns, and developing governance and accountability mechanisms.

Of the current approaches, the most common has been the creation of temporary, quasi-government bodies (e.g., commissions or task forces), which include both external experts and government workers. These bodies are tasked with examining emerging technologies and publishing their findings, along with recommendations for how ADS systems should be held accountable.

To date, this approach has primarily been implemented by jurisdictions in the United States. Alabama, New York City, and Vermont have already commenced their respective commissions and task forces, and legislation seeking to create similar bodies is pending in Massachusetts,

Washington, and New York State.[247] This follows a tradition in the US, in which task forces and similar bodies convene when the government is facing emerging or controversial issues. With the credibility offered by non-governmental experts, task forces (and similar) develop new strategies, policies, standards, or guidance that can inform future legislation or regulation.The New York City Automated Decision Systems Task Force was the first of these quasi-government bodies to complete its mandate; however, the process revealed missed opportunities in New York City that should be avoided in Vermont, Alabama, and other jurisdictions considering quasi-government bodies as a policy intervention.

The NYC Task Force's shortcomings include a significant lack of public engagement and the city's central role in drafting the NYC ADS Task Force Report, which produced a document that did not reflect Task Force consensus, and was biased in favor of city ADS use. In addition, the law enforcement carveout, which was reflected in both the report and an Executive Order issued by the Mayor's office, presents a significant omission. Law enforcement's use of automated decision systems, from facial recognition to predictive policing and beyond, poses some of the greatest threats to residents, and must be included in any oversight of automated decision systems. On November 19, 2019, Mayor Bill de Blasio released the ADS Task Force Report along with an executive order to establish an Algorithms Management and Policy Officer within the Mayor's Office of Operations.[248] On November 26, 2019, Council Member Peter Koo introduced legislation that requires annual reporting on ADS used by city agencies. A more detailed account of the missed opportunities and lessons learned from the NYC ADS Task Force Process, in addition to recommendations for other jurisdictions, can be found in *Confronting Black Boxes: A Shadow Report of the New York City Automated Decision System Task Force.*[249]

Litigation Is Filling Some of the Void

This year, various coalitions also continued their attempts to use litigation to hold both governments and vendors accountable for harmful uses of AI.[250]

For example, Disability Rights Oregon (DRO) sued the state's Department of Human Services over sudden cuts in Oregonians' disability benefits with no notice or explanation. In the investigation and litigation process, DRO discovered that the reduction was due to the State hard-coding a 30-percent across-the-board reduction of hours into their algorithmic assessment tool. The State quickly accepted a preliminary injunction that restored all recipients' hours to their prior levels, and agreed to use the previous version of the assessment tool going forward. Yet, much like previous cases in Idaho and Arkansas,[251] although the Oregon injunction put that particular AI system out of service, it is unclear exactly what the State will offer in its place, and how they will implement it.

In Michigan, a group of unemployment beneficiaries brought a class-action lawsuit against the Michigan Unemployment Insurance Agency (UIA) over a failed automation project, called MiDAS, that claimed to be able to detect and "robo-adjudicate" claims of benefits fraud algorithmically. The state hired third-party tech vendors to build the system, requesting they design it to

automatically treat any data discrepancies or inconsistencies in an individual's record as evidence of illegal conduct. Between October 2013 and August 2015, the system falsely identified more than 40,000 Michigan residents of suspected fraud. The consequences were severe: seizure of tax refunds, garnishment of wages, and imposition of civil penalties—four times the amount people were accused of owing. And although individuals had 30 days to appeal, that process was also flawed.

These events prompted a class-action lawsuit filed in state court in 2015 alleging due-process violations. After a lower court decision denied the claim, the Michigan Supreme Court reversed in 2019 to allow the case to proceed to trial. In the meantime, Michigan continues to use MiDAS, and claims that adjudications are no longer fully automated. It is unclear what (if any) changes were made, and whether there is any meaningful human review or oversight.

2. EMERGING AND URGENT CONCERNS IN 2019

2.1 The Private Automation of Public Infrastructure

As attention to the concerns about AI infrastructures increases, we tend to see them discussed in terms of a dichotomy between public and private uses. This separation has always been false on some level and this year we have seen signs of its eventual collapse, with clear evidence of ongoing and expansive integration of public and private systems across many different AI domains.

AI and Neighborhood Surveillance

Troubling partnerships between government and private tech companies also emerged as a trend this year, especially those that extended surveillance from public environments into private spaces like private properties and the home.

For example, this summer, a Canadian RCMP troop in Red Deer, Alberta, launched a program called CAPTURE to enable "community assisted policing through the use of recorded evidence."[252] The idea was for commercial businesses and personal residences with private security-camera infrastructure to effectively share the captured information on their private property with the police, under the guise of improved community safety. As of November, more than 160 properties are participating, effectively covering the entire map of the city, and providing access to the police surveillance of spaces previously inaccessible without a warrant and consent for entry.[253] Since 2016, Project Green Light in the City of Detroit in the United States has been working in an almost identical fashion. By March of 2019, the mayor of Detroit decided to establish the "Neighborhood Real-Time Intelligence Program," described as "a $9 million, state- and federally-funded initiative

that would not only expand Project Green Light by installing surveillance equipment at 500 Detroit intersections—on top of the over 500 already installed at businesses—but also utilize facial recognition software to identify potential criminals."[254]

Amazon exemplified this new wave of commercial surveillance tech with Ring, a smart-security-device company acquired by Amazon in 2018. The central product is its video doorbell, which allows Ring users to see, talk to, and record those who come to their doorsteps. This is paired with a neighborhood watch app called "Neighbors," which allows users to post instances of crime or safety issues in their community and comment with additional information, including photos and videos.[255] A series of reports reveals that Amazon had negotiated Ring video-sharing partnerships with more than 700 police departments across the US. Partnerships give police a direct portal through which to request videos from Ring users in the event of a nearby crime investigation.[256] Not only is Amazon encouraging police departments to use and market Ring products by providing discounts, but it also coaches police on how to successfully request surveillance footage from Neighbors through their special portal.[257] As Chris Gilliard, a professor who studies digital redlining and discriminatory practices, comments: "Amazon is essentially coaching police on . . . how to do their jobs, and . . . how to promote Ring products."[258]

Neighbors is joined by other apps like Nextdoor and Citizen, which allow users to view local crime in real time and discuss it with one another. Ring, Nextdoor, and Citizen have all been criticized for feeding into existing biases around who is likely to commit crime; Nextdoor even changed its software and policies given extensive evidence of racial stereotyping on its platform.[259] Others see these app-based surveillance operations sowing a climate of fear, while tech companies profit from a false perception that crime is on the rise.[260]

Smart Cities

Concerns about the privatization of public space took center stage this year in the debate around "smart cities" (municipalities that use data, sensors, and algorithms to manage resources and services).

Most smart-city initiatives rely on public-private partnerships and technology developed and controlled by tech companies, which shifts public resources and control over municipal infrastructure and values to these companies.[261] Recent research has exposed the extent to which major tech companies such as IBM and Cisco have been "selling smartness" by disseminating narratives about urban challenges and technological solutions to those challenges.[262] The Alphabet company Sidewalk Labs has similarly been producing vision documents replete with renderings of utopian urban scenes.[263] These companies see the potential for massive profits: one report estimated the global smart cities market being worth $237.6 billion by 2025.[264]

Smart-city projects around the United States and the world increasingly consolidate power in the hands of for-profit technology companies, while depriving municipalities and their residents of resources and privacy. The highest-profile example is in Toronto, the home of Sidewalk Lab's project to develop "the world's first neighbourhood built from the internet up."[265] A report in February 2019 found that Sidewalk Labs has expressed a desire to receive a portion of the property taxes and development fees (estimated at $30 billion over 30 years) associated with the project, which would otherwise go to the City of Toronto.[266] And in June 2019, Sidewalk Labs released a Master Innovation and Development Plan (MIDP), describing plans to develop and manage a far larger plot of land than the 12 acres for which the company was initially given license to develop plans.[267]

Smart-city projects also lack transparency and genuine forms of civic participation.[268] Sidewalk Labs's civic engagement efforts have been described as a process of obfuscation and "gaslighting."[269] Similarly, a contract between urban-planning software company Replica (a Sidewalk Labs spinoff company) and the Portland, Oregon regional transportation planning agency provides no public access to Replica's algorithms.[270] Siemens is launching a €600 million smart-city neighborhood in Berlin, creating "laboratories in reality" with barely any public meetings so far.[271]

Many of these public-private partnerships directly enhance the government's surveillance capabilities. Chicago and Detroit have both purchased software enabling them to deploy facial recognition in the video feeds from cameras across the cities.[272] Similarly, the multinational Chinese tech company Huawei's $1.5 billion project to create smart cities in Africa[273] included a project in Nairobi where it installed 1,800 cameras, 200 traffic surveillance systems, and a national police command center as part of its "Safe City" program.[274] Huawei's Safe City technology has been used by some African governments to spy on political opponents.[275]

In other cities, behind-the-scenes data-sharing arrangements allow data collected by private companies to flow into law-enforcement agencies. San Diego has installed thousands of microphones and cameras on street lamps in recent years in an effort to study traffic and parking conditions; although the data has proven of little use in improving traffic, the police have used the video footage in more than 140 cases without any oversight or accountability.[276] The City of Miami is actively considering a 30-year contract with Illumination Technologies, providing the company with free access to set up light poles containing cameras and license-plate readers, collecting information that will filter through the Miami Police Department (and that the company can use in unchecked ways).[277] Documents obtained via public-records requests showed that 300 police departments in California have access, through Palantir, to data collected and stored by the Department of Homeland Security's Northern California Regional Intelligence Center, without any requirement to disclose their access to this information.[278]

Numerous groups are beginning to push back on the encroaching privatization fueled by smart cities, with the most concerted and organized effort in Toronto. In February, a group of 30 Torontonians launched the #BlockSidewalk campaign,[279] and has noted that the project "is as

much about privatization and corporate control as it is about privacy."[280] In April, the Canadian Civil Liberties Association (CCLA) filed a lawsuit against Waterfront Toronto, arguing the organization abused its legal authority in granting Sidewalk Labs the authority to develop data-governance policy.[281] And after Sidewalk Labs released its MIDP, the Chairman of Waterfront Toronto (the government task force charged with managing the Sidewalk Labs project) critiqued the proposal in a public letter as "premature."[282]

By the end of October, Waterfront Toronto had reached a new agreement with Sidewalk Labs, restricting Sidewalk Labs to the original 12-acre parcel and asserting the government's role as leading key components of the project.[283] The project's ultimate fate is still undetermined: Waterfront Toronto continues to review the project and will come to a final decision about whether to proceed by March 31, 2020.[284]

AI at the Border

AI continues to play a larger and more pernicious role in the targeting of immigrant populations within the United States.

The increasing use of AI technologies is often justified based on nationalist rhetoric. In the US, talk of a "smart wall" that utilizes drones, sensors, and increased facial recognition to detect individuals is receiving bipartisan support in design and implementation.[285] Anduril Industries, a technology company that recently replaced Google on a Project Maven Department of Defense contract developing AI-based surveillance systems and that also produces autonomous drones,[286] now provides solar-powered "sentry" towers for the Customs and Border Protection (CBP) agency.[287] One of Anduril's earliest investors, Peter Thiel, also founded the company Palantir Technologies, which provides database management and AI to ICE. Palantir's tech has enabled agencies such as ICE to combine and analyze information from varying government databases, and to use this to track, target, and detain people whom they believe are in the US "illegally."[288] In July, the *Washington Post* reported on thousands of internal documents and emails obtained through public-records requests by researchers at Georgetown Law's Center on Privacy and Technology. The documents showed that the Federal Bureau of Investigation (FBI) and ICE were using state driver's license databases as "the bedrock of an unprecedented surveillance infrastructure" that relied on facial-recognition technology.[289] The US Justice Department also recently announced plans to collect DNA data from migrants crossing the border, which could create more invasive monitoring of immigrants without any real limits.[290]

Outside the US, governments are equally eager to pilot AI systems at border checkpoints. The EU aims to deploy an AI-based "lie detector" built by iBorderCtrl, but makes no mention of the predictive accuracy or the inherent bias that might exist within such tools.[291] In the UK, the Home Office facial-recognition systems were found to be wrongfully identifying travelers as criminals, delaying their travels and detaining them with no elements of due process.[292] Meanwhile, some US-based technology companies have been found to be deploying these faulty security solutions

outside of the US. Journalists recently revealed that Microsoft funded an Israeli firm to conduct facial-recognition surveillance on West Bank Palestinians in public space.[293] China, having already built massive surveillance capital to track and identify citizens anywhere in the country and beyond, now also employs affect recognition to try to identify criminals at airports and subway stations.[294]

The significant growth in AI use for border tracking, surveillance, and prediction threatens the rights and civil liberties of residents within a country's borders, not only those outside of it. In the US, such technologies act as force multipliers for ICE and CBP, amplifying their ability to track and target immigrants and residents. Such powers are extended well beyond the border between the US and Mexico, and often do so at the expense of constitutional rights. The US border zone consists of a hundred-mile band, from the border inland, tracing the whole of the US. Nearly two-thirds of US residents live within it. As the ACLU says in their analysis of the problems with CBP's authority within the US border zone: "The spread of border-related powers inland is inseparable from the broader expansion of government intrusion in the lives of ordinary Americans."[295] And as AI-enabled surveillance, tracking, and targeting in the context of border security become more pervasive and more powerful, such technologies will inevitably be used on US residents, further infringing on rights and liberties within the country.

National Biometric Identity Systems

An increasing number of governments across the world are building national biometric identity systems that generate a unique identifier for each person, typically serving as a link to discrete government databases. Residents in many countries are increasingly required to use these new digital modes in order to access a range of services. Along with demographic information, biometrics like fingerprints, iris scans, or facial scans are used either for one-time enrollment into an ID database or as a continuing means of authentication. These ID systems vary in terms of whom they are meant to include (and exclude): residents, citizens, or refugees.[296] Many of these projects are in countries in the global South and have been actively encouraged as a development priority by organizations like the World Bank under the "ID4D" banner[297] and supported as fulfilling the UN Sustainable Development Goals.[298] Although these projects are often justified as creating efficiencies in the rollout of government services to benefit the "end user," they appear to more directly benefit a complex mix of state and private interests.

India, for example, introduced a national ID to supposedly create more efficient welfare distribution that also happened to be designed for market activity and commercial surveillance.[299] Until intervention by the Indian Supreme Court,[300] any private entity was allowed to use the state's biometric ID infrastructure for authentication, including banks, telecom companies, and a range of other private vendors with little scrutiny or privacy safeguards. A recent report[301] describes how ID databases in Ghana, Rwanda, Tunisia, Uganda and Zimbabwe are facilitating "citizen scoring" exercises like credit reference bureaus to emerge at scale.

The involvement of foreign technology vendors for key technical functions has also raised serious national-security concerns in Kenya[302] and India. There have already been multiple attempts at breaching these ID databases,[303] and there was a security flaw in the Estonian ID system, which was otherwise celebrated as a technically advanced and privacy-respecting model.[304] A security breach of the biometrics in these databases could potentially create lifelong impacts for those whose bodily information is compromised.

The dossiers of authentication records created by these ID systems, as well as the ability to aggregate information across databases, can increase the power of surveillance infrastructures available to governments. Kenya's Home Minister referred to its recently announced biometric ID system "Huduma Numba" as creating a "single source of truth" about each citizen.[305]

Enrollment and associated data collection for these ID systems has been coercive because it is either de facto or legally mandatory to be enrolled to access essential services. These instances must be understood against the backdrop of claims that these systems will create cost savings by weeding out fake or "ghost"[306] beneficiaries of welfare services, which replays the familiar logic of using technical systems as a way to implement and justify austerity policies.[307] In India and Peru, multiple cases of welfare-benefits denials led to higher malnutrition levels[308] and even starvation deaths[309] because people either were not enrolled or were unable to authenticate due to technical failures.

There is growing concern about the assumed efficiency of these automated systems, as well as about whom these technical systems benefit and at what cost. This year, the Jamaican Supreme Court struck down[310] Jamaica's centralized, mandatory biometric ID system, noting that the project led to privacy concerns that were "not justifiable in a free and democratic society." Soon after, Ireland's Data Protection Commissioner ordered the government to delete the ID records of 3.2 million people after it was discovered that the new "Public Services Card" was being used without limits on data retention or sharing between government departments.[311] After years of civil society protest and strategic litigation against the Indian biometric ID system Aadhaar, the Indian Supreme Court put several limits on the use of the system by private companies (although it has permitted large-scale and coercive government use).[312] The Kenyan Supreme Court is currently hearing multiple constitutional challenges to Huduma Namba, the national ID system that proposes to collect a range of biometrics including facial recognition, voice samples, and DNA data.[313]

These moments of backlash have not deterred other governments and donor agencies from pushing similar centralized biometric ID systems elsewhere. Just this October, the Brazilian government announced its intention to create a centralized citizen database for every resident, involving the collection of a wide range of personal information, including biometrics.[314] France has announced that it will trial facial scans to enroll citizens in its latest national ID venture.[315]

As these projects continue to emerge across the world, more research into the international political economy of these ID systems is required. Civil society coalitions like the #WhyID

campaign[316] are coming together to fundamentally question the interests driving these projects nationally and through international development organizations, as well as developing advocacy strategies to influence their development.[317]

China AI Arms Race Narrative

In the last couple of years, the "AI arms race" between the US and China (and to a lesser extent Russia) has become a frequent topic of public discourse.[318] This "race" is commonly cited as a reason the US and the tech companies that produce the country's AI systems need to ramp up AI development and deployment and push back against calls for slower, more intentional development and stronger regulatory protections.

It is important to question the role that the "AI arms race" narrative plays in the discourse around AI. Who is driving it, and what interests and power structures do they represent? Critically, what futures do they guide us toward? And on what basis are these claims founded, and how is "progress" in such a race measured?

Metrics comparing US and China AI development often focus on the proportion of top AI scientists and engineers who reside and work in each country, whether Chinese or US researchers authored the most cited technical papers, or how many AI patents emerged from each country.[319] Based on such evidence, recent studies have warned that China could "overtake" the United States in this measure by 2020,[320] with others warning that top AI scientists from Silicon Valley are emigrating to China to join competing Chinese companies.[321]

While China and the US are certainly leading based on these measures of technical AI development, with profound geopolitical implications, it's also important to look at what these measures omit. Empirical factors like where AI produced in either country will eventually be deployed, what purpose such systems will be put to, whether they work, and which communities bear the risk of bias and other harms are rarely discussed within the "arms race" discourse. Given the mounting evidence of harm due to AI systems being applied in sensitive social contexts, these questions are urgent. And yet they are not being considered in the current estimation of which country is "winning" the "AI race." Asking such questions can help assess the goals of "the arms race" itself, and what the implications of "winning" the race might be.

Proponents of the AI arms race narrative also tend to measure "progress" based on AI-industry cooperation with the military establishment, characterizing the reticence of those who would question the development of weapons systems and mass surveillance systems as implicitly "anti-progress" or unpatriotic. Indeed, some of the most consistent voices warning of the dangers of Chinese AI supremacy come from within the US defense establishment.[322] This fits with the growing attention to the military use of AI, and the call for increased military spending on AI and closer partnerships between the US military and Silicon Valley.[323]

Chinese tech companies' purported willingness to work on weapons and military technology is frequently contrasted with the US, where tech workers, human rights groups, and academics have pushed back against Silicon Valley companies entering into contracts with US military efforts (such as opposition within Google to Project Maven).[324] Such resistance to privatized, AI-enabled weapons and infrastructure is seen as causing unjustified friction in this race.[325] Former Secretary of Defense Ashton Carter said that it was "ironic" that US companies would not be willing to cooperate with the US military, "which is far more transparent [than the Chinese] and which reflects the values of our society."[326]

More broadly, this view of progress tends to see all calls for restraint, reflection, and regulation as a strategic disadvantage to US national interest. It turns accountability into a barrier to progress and suppresses calls for oversight.[327] At a time when "move fast and break things" is acknowledged to have done long-term harm to core social and political infrastructures, this emphasis on speed seems particularly misplaced.

The urgency of "beating" China is commonly justified based on the nationalist assumption that the US would imbue its AI technologies, and its application of said technologies, with better values than China would. China's authoritarian government is presumed to promote a more dystopian technological future than Western liberal democracies.

The Chinese government's oppression of minorities through state-private partnerships (including a significant reliance on US technology) is well documented and rightly condemned by human rights organizations.[328] Yet, China's use of AI should serve as a warning to the US of what can happen when you put technological "progress" above human rights and civil liberties. And there is growing evidence that the US is increasingly using AI in oppressive and harmful ways that echo China's use. Scholars like Shazeda Ahmed[329] and Abeba Birhane[330] point out that many elements of Chinese AI technology are actually commonplace in the US digital economy. However, such applications of AI in the US are frequently enabled by private AI companies, from Amazon selling facial recognition to law enforcement to Palantir providing surveillance and tracking infrastructure to ICE. Such uses are often protected by contractual secrecy, and not disclosed as state policy. And when they are exposed, it's generally by whistleblowers and investigative journalists, not by the companies or agencies partnering to develop and apply these AI systems.

2.2 From "Data Colonialism" to Colonial Data

The Abstraction of "Data Colonialism" and Context Erasure

"Data colonialism" and "digital colonialism" have become popular metaphors for academics,[331] policymakers, and advocacy organizations looking to critique harmful AI practices. In these accounts, colonialism is generally used to explain the extractive and exploitative nature of the relationship between technology companies and people, deployed toward varying political ends.

In Europe, for example, it is used by advocacy groups to argue for a movement toward "digital sovereignty" that encourages decentralized and community-owned data-governance mechanisms.[332] In India, domestic industrialists and policymakers have argued that Silicon Valley tech giants are "data colonizers" and that national companies, rather than foreign ones, must get first priority accessing Indians' data.[333]

However, using data colonialism as a metaphor to abstract tech company practices overlooks specific historical, cultural, and political contexts and obscures the fact that present-day AI labor and economic structures exist *because of* actual histories of colonization.[334] Growing research on the locally specific real-world impact of the AI industry on countries in the global South makes visible these contexts and the lived human conditions behind the technology and data.[335] As demonstrated by policy narratives in India, abstracting "colonialism" can allow narrow economic interests to co-opt the rhetoric of decolonial struggles while replicating the same extractivist logics of their Silicon Valley counterparts. This has led to a growing critique of these metaphorical usages,[336] and a need to recenter the narrative on lived experiences to build broader solidarity with communities directly affected by AI.

Colonial Data: Statistics and Indigenous Data Sovereignty

Indigenous communities have been at the forefront of resisting harms caused by data abstraction.[337] For example, advocacy groups have drawn attention to the ways that census information and population counts function[338] as a core feature of settler-colonial governance, feeding massive amounts of abstracted data into digital systems.[339] Problematic uses of such "Indigenous statistics" in census administration directly link to underrepresentation and the lack of resources these communities face.[340]

In the context of open-data movements, a number of Indigenous-led movements for sovereignty and self-determination over data and data analysis have emerged. The term "Indigenous data sovereignty" (ID-Sov) is generally defined as "the right of a nation to govern the collection, ownership, and application of its own data."[341] The term data sovereignty, like data colonialism, is currently used by both Indigenous and non-Indigenous policy and advocacy groups to make appeals in data ownership and proprietary rights, but with very different historical, social, and political contexts.[342]

These groups have implemented new programs, organizational frameworks, and data policy to address Indigenous data sovereignty and data governance across local, national, and transnational contexts. In 2016, the US Indigenous Data Sovereignty Network (USIDSN) was established to "link American Indian, Alaska Native, and Native Hawaiian data users, tribal leaders, information and communication technology providers, researchers, policymakers and planners, businesses, service providers, and community advocates together to share stories about data initiatives, successes, and challenges, and resources." The same year, a collective of Māori scholars and government leaders and Aboriginal rights developers published the book Indigenous

Data Sovereignty: Toward an Agenda in response to oversights in the United Nations Declaration on the Rights of Indigenous Peoples (UNDRIP).[343]

The Indigenous Data Sovereignty program set forth to address "the twin problems of a lack of reliable data and information on indigenous peoples and biopiracy and misuse of their traditional knowledge and cultural heritage."[344]

Advocacy groups are establishing sovereignty and ownership protocols at the level of data and analysis.[345] For example, the Local Contexts initiative aims to support Native, First Nations, Aboriginal, Inuit, Metis, and Indigenous communities in the management of their intellectual property and cultural heritage in the growing digital environment.[346] Their Traditional Knowledge or TK labels are "designed as a tool for Indigenous communities to add existing local protocols for access and use to recorded cultural heritage that is digitally circulating outside community contexts."[347] TK labels are a framework for labeling data through local decision and preserved in circulation and exchange. The US Library of Congress has recently integrated TK labels to digitally reformat older media formats "to recover and preserve the recorded voices and languages of Native American people."[348] More than an archival process, Local Contexts is working toward "a new paradigm of rights and responsibilities that recognizes the inherent sovereignty that Indigenous communities have over their cultural heritage." This moves toward the possibility of reconfiguring entire information systems, like the US Library of Congress, according to Indigenous sovereignty guidelines.[349]

In September, the Global Indigenous Data Alliance (GIDA) launched.[350] Responding directly to the international open-data and open-science debates, GIDA has put forward a set of "CARE principles" that address the power differentials and historical contexts neglected by the open-data movements' "FAIR principles," which value data as "findable, accessible, interoperable, reusable."[351] GIDA aims to establish internationally recognized protocols of meaning for local Indigenous data and to assert values for data generation, circulation, and application beyond the culturally flattening notion of open accessibility. GIDA's data CARE principles are Collective benefit, Authority to control, Responsibility, and Ethics.

2.3 Bias Built In

While Indigenous peoples are calling for data sovereignty and bringing attention to the thorny relationships among how individuals are defined by data and the resources allocated to them, the same set of issues has recently played out on the national American stage, prompting investigations and calls for reform.

In November, the prominent software engineer and author David Heinemeier Hansson propelled a renewed wave of criticism of algorithmic discrimination with his tweet about the Apple Card. He castigated Apple because he received a credit limit 20 times higher than his wife, Jamie

Heinemeier Hansson.[352] Meanwhile, Apple cofounder Steve Wozniak's wife, Janet Hill, was allocated a credit limit that was a mere 10 percent of her husband's.[353] Ultimately, Hansson's complaint about the sexist Apple Card algorithms triggered investigations by both the Senate Committee on Finance and the New York State Department of Financial Services.[354]

Hansson blamed a sexist black-box algorithm, echoing and amplifying the work of numerous activists, journalists, researchers, and tech workers (like Hansson himself) who have been warning of the dangers of biased AI systems for at least a decade.[355] Many of those pioneering this work are people of color, and they predominantly identify as women or non-binary. They have rigorously researched, detected, and proved bias in advertising networks, facial recognition, search engines, welfare systems, and even algorithms used in criminal sentencing.

However, the tech industry—which by contrast is predominantly led by white, wealthy men[356]—has been doing its best to resist, minimize, and even mock this critical and alarming work. Hansson himself observed the denialism in the responses to his tweet criticizing the Apple Card. He commented: "Every single poster questioning my wife's credit score, a man. Every single defense of Apple blaming G[oldman] S[achs], a man. Almost like men are over represented in the defense/justification of discrimination that doesn't affect them?"[357] Indeed, Hansson had encapsulated the defensiveness of Google Chairman Eric Schmidt speaking at Stanford University late in October; Schmidt groused, "We know about data bias. You can stop yelling about it."[358]

Although Schmidt's comment appeared offhand, it served to underscore that tech companies are, in fact, deeply aware that algorithmic discrimination is entrenched in the systems with which they are blanketing the world. In fact, Microsoft's latest report to shareholders flagged reputational harm due to biased AI systems among the company's risks.[359] Although the industry is proffering ostensible solutions such as corporate AI ethics, those solutions are failing, as discussed elsewhere in this report. So far, Big Tech refuses to prioritize solving these issues over their bottom line.

Recent research has highlighted how the bias built into the tech industry works in a feedback loop from a dire lack of diversity among employees to damaging discrimination embedded in algorithms.[360] One study found that only 18 percent of speakers at leading AI conferences were women,[361] while another showed that 80 percent of AI professors are men.[362] Indicators suggest that things look much worse when considering representation by race, ethnicity, or ability.[363] Such diversity of experience is a fundamental requirement for those who develop AI systems to identify and reduce the harms they produce.[364]

Just as the so-called solution of corporate AI ethics is no solution at all, the so-called solution to "diversity in tech" often centers simply around highly visible "Women in Tech" initiatives that privilege white women above others.[365] But the challenges go far beyond this, from barriers to entry to toxic experiences within AI spaces.[366] In fact, a recently released documentary, *Losing Lena,* highlights the five-decade-long history of how an image of a nude woman has continued to

be used in the tech industry, pointing to "the many small ways in which women (and . . . people of color) are told they do not belong in the tech industry."[367]

What would it look like to expand the frame? For one, attending to the experiences of communities who have been erased from the field of AI does much more than foster inclusion or help identify where technologies produce biased outcomes. It also surfaces new ways of understanding how technological systems order our social world. The work of disability scholars and activists has much to offer in explaining both the processes and consequences of erasure.[368] Disability scholarship also emphasizes that the concept of "normal," and the tools and techniques for its enforcement, has historically constructed the disabled body and mind as deviant and problematic. Scholars in this area may consider how we can better assess the normative models encoded in AI systems, and what the consequences of enforcing these norms may be (and for whom).

The integration of community voices and stories at only a surface level is all too often used as a marketing strategy, mobilized to support practices that are ultimately not in service of community needs. In attending to affected communities it is crucial that their needs be centered, in their own voices. As the credo of the disability rights movement puts it: "Nothing about us, without us." It is critical that participation in the work of actively resisting discrimination in the field be seen as the responsibility of everyone, and that the labor of resistance not be left solely to those who are most affected by the harms of AI.

2.4 AI and the Climate Crisis

On September 20, workers from 12 tech companies joined the global climate strike.[369] They highlighted tech's role in climate change and demanded "zero carbon emissions by 2030, zero contracts with fossil fuel companies, zero funding of climate denial lobbying or other efforts, and zero harm to climate refugees and frontline communities."[370]

This might have surprised some people, as tech's contribution to the climate crisis is rarely acknowledged. Indeed, industry marketing often highlights green policies, sustainability initiatives, and futures in which AI and other advanced technologies provide solutions to climate problems. But the tech sector is a significant contributor to climate change and environmental harms.[371]

AI Makes Tech Dirtier

The tech industry faces criticism for the significant energy used to power its computing infrastructure. As a whole, the industry's energy dependence is on an exponential trajectory, with best estimates showing that its 2020 global footprint amounts to 3.0–3.6 percent of global greenhouse emissions, more than double what the sector produced in 2007.[372] This is

comparable to that of the aviation industry,[373] and larger than that of Japan, which is the fifth biggest polluter in the world.[374] In the worst-case scenario, this footprint could increase to 14 percent of global emissions by 2040.

In response, the major tech companies have made data centers more efficient, and have worked to ensure they're powered at least in part by renewable energy—changes they're not shy about, announcing them with marketing blasts and much public fanfare.[375] These changes are a step in the right direction, but don't come close to tackling the problem. Most large tech companies continue to rely heavily on fossil fuels, and when they do commit to efficiency goals, these are most often not open to public scrutiny and validation.[376][377]

The AI industry is a significant source of further growth in greenhouse emissions. With the emergence of 5G networks aiming to realize the "internet of things," the increased acceleration of data collection and traffic is already underway.[378] In addition to 5G antennas consuming far more energy than their 4G predecessors,[379] the introduction of 5G is poised to fuel a proliferation of carbon-intensive AI technologies, including autonomous driving[380] and telerobotic surgery.[381]

A core contributor to the AI field's growing carbon footprint is a dominant belief that "bigger is better." In other words, AI models that leverage massive computational resources to consume larger training datasets are assumed to be inherently "better" and more accurate.[382] While this narrative is inherently flawed,[383] its assumptions drive the use of increased computation in the development of AI models across the industry.

Last year, researchers Dario Amodei and Danny Hernandez at OpenAI reported that "[s]ince 2012, the amount of [computation] used in the largest AI training runs has been increasing exponentially with a 3.4 month doubling time (by comparison, Moore's Law had an 18 month doubling period)."[384] Their observations show developers "repeatedly finding ways to use more chips in parallel, and . . . willing to pay the economic cost of doing so".

As AI relies on more computers, its carbon footprint increases, with significant consequences. A recent study from the University of Massachusetts, Amherst estimated the carbon footprint of training a large natural-language processing model. Emma Strubell and her coauthors reported that training just one AI model produced 300,000 kilograms of carbon dioxide emissions.[385] That's roughly the equivalent of 125 round-trip flights from New York to Beijing.

AI and the Fossil Fuel Industry

Adding to their already sizeable climate impact, big AI companies are aggressively marketing their (carbon-intensive) AI services to oil and gas companies, offering to help optimize and accelerate oil production and resource extraction. Amazon is luring potential customers in the oil and gas industry[386] with programs like "Predicting the Next Oil Field in Seconds with Machine Learning."[387] Microsoft held an event called "Empowering Oil & Gas with AI,"[388] and Google Cloud has its own

energy vertical dedicated to working with fossil fuel companies.[389] And C3 IoT, an AI company originally created to facilitate the transition to a society fueled by renewable energy, now helps large oil and gas companies, including Royal Dutch Shell, Baker Hughes, and Engie, to expedite their extraction of fossil fuel.[390]

A recent article in *Logic* points out that oil and gas account for 30 percent of the total addressable market, making "the success of Big Oil, and the production of fossil fuels . . . key to winning the cloud race."[391] Recently, the *Guardian* examined the role of Big Tech in sustaining the market for fossil fuel, illuminating the massive amounts of money tech companies invest in organizations that actively campaign against climate legislation, and promote climate change denial.[392]

Opacity and Obfuscation

When researchers and policymakers attempt to account for tech's climate footprint, it is immediately clear how little information is available. They are left to rely on voluntary company disclosures, without access to the information they would need to make a thorough accounting of tech's true energy use.

There is very little public data available, and few incentives for tech companies to release it. Without the information necessary to reach robust conclusions, researchers Lotfi Belkhir and Ahmed Elmeligi had to estimate 2018 data-center energy consumption using data from 2008.[393] It was all they had to work with, even though, over the past ten years, both the scale of computation and the technologies powering it have changed radically.

The authors of Greenpeace's report make similar observations, stating that while efficiency metrics have been eagerly adopted by the industry, "very few companies report under newer metrics . . . that could shed any light on the basic question: how much dirty energy is being used, and which companies are choosing clean energy to power the cloud?"[394] More frustratingly, the unwillingness of cloud providers to provide customers with insight into the energy use of procured services forms a critical barrier to meaningful carbon accounting across all sectors and organizations that rely on digital technology.

2.5 Flawed Scientific Foundations

Concerns about AI systems focus not only on the harms caused when they are deployed without accountability; they also include the underlying and often flawed scientific foundations upon which they are built and then marketed to the public. This year, researchers uncovered systems in wide deployment that purport to operationalize proven scientific theories, but in the end are little more than speculation.[395] This trend in AI development is a growing area of concern, especially as applied to facial- and affect-recognition technology.

Facial/Affect Recognition

Affect recognition is an AI-driven technology that claims to be able to detect an individual's emotional state based on the use of computer-vision algorithms to analyze their facial microexpressions, tone of voice, or even their gait. It is rapidly being commercialized for a wide range of purposes—from attempts to identify the perfect employee[396] to assessing patient pain[397] to tracking which students are being attentive in class.[398] Yet despite the technology's broad application, research shows affect recognition is built on markedly shaky foundations.

The affect-recognition industry is undergoing a period of significant growth: some reports indicate that the emotion-detection and -recognition market was worth $12 billion in 2018, and by one enthusiastic estimate, the industry is projected to grow to over $90 billion by 2024.[399] These technologies are often layered on top of facial-recognition systems as a "value add."

For example, the company Kairos is marketing video-analytics cameras that claim to detect faces and then classify them as feeling anger, fear, and sadness, along with collecting customer identity and demographic data. Kairos sells these products to casinos, restaurants, retail merchants, real estate brokers, and the hospitality industry, all with the promise that they will help those businesses see inside the emotional landscape of their patrons.[400] In August, Amazon claimed its Rekognition facial recognition software could now assess fear in addition to seven other emotions. Though it declined to provide any details on how it is being used by customers, it indicated retail as a potential use case, illustrating how stores can feed live images of shoppers to detect emotional and demographic trends.[401]

Employment has also experienced a surge in the use of affect recognition, with companies like HireVue and VCV offering to screen job candidates for qualities like "grit" and to track how often they smile.[402] Call center programs Cogito and Empath use voice-analysis algorithms to monitor the reactions of customers and signal to call agents when they sound distressed.[403] Similar programs have been proposed as an assistive technology for people with autism,[404] while Boston-based company BrainCo is creating headbands that purport to detect and quantify students' attention levels through brain-activity detection,[405] despite studies that outline significant risks associated with the deployment of emotional AI in the classroom.[406]

Affect-recognition software has also joined risk assessment as a tool in criminal justice. For example, police in the US and UK are using the eye-detection software Converus, which examines eye movements and changes in pupil size to flag potential deception.[407] Oxygen Forensics, which sells data-extraction tools to clients including the FBI, Interpol, London Metropolitan Police, and Hong Kong Customs, announced in July it also added facial recognition, including emotion detection, to its software, which includes "analysis of videos and images captured by drones used to identify possible known terrorists."[408]

But often the software doesn't work. For example, ProPublica reported that schools, prisons, banks, and hospitals have installed microphones from companies that carry software developed by the company Sound Intelligence, purporting to detect stress and aggression before violence erupts. But the "aggression detector" was not very reliable, detecting rough, higher-pitched sounds like coughing as aggression.[409] Another study by researcher Dr. Lauren Rhue found systematic racial biases in two well-known emotion-recognition programs: when she ran Face++ and Microsoft's Face API on a dataset of 400 NBA player photos, she found that both systems assigned black players more negative emotional scores on average, no matter how much they smiled.[410]

There remains little to no evidence that these new affect-recognition products have any scientific validity. In February, researchers at Berkeley found that in order to detect emotions with accuracy and high agreement requires context beyond the face and body.[411] Researcher Ruben van de Ven makes this point in his exploration of affect recognition, citing the "Kuleshov Effect," an experiment from the beginning of the twentieth century in which filmmaker Lev Kuleshov "edited three video sequences. Each sequence showed the same 'neutral' face of a man, followed by the image of a dead man, a plate of soup or a woman . . . . When these sequences were shown, the audience 'raved about the acting', believing the man who 'looked' at the dead man, the soup or the woman, was either expressing grief, hunger or desire."[412] Others at the University of Southern California called for a pause in the use of some emotion analytics techniques at the 8th International Conference on Affective Computing and Intelligent Interaction this year. "'[T]his facial expression recognition technology is picking up on something — it's just not very well correlated with what people want to use it for. So they're just going to be making errors, and in some cases, those errors cause harm,'" said Professor Jonathan Gratch.[413]

A major review released this summer found that efforts to "read out" people's internal states from an analysis of facial movements alone, without considering context, are at best incomplete and at worst entirely lack validity.[414] After reviewing over a thousand studies on emotion expression, the authors found that, although these technologies claim to detect emotional state, they actually achieve a much more modest outcome: detecting facial movements. As the study shows, there is a substantial amount of variance in how people communicate their emotional state across cultures, situations, and even across people within a single situation. Moreover, the same combination of facial movements—a smile or a scowl, for instance—can express more than a single emotion. The authors conclude that "no matter how sophisticated the computational algorithms . . . it is premature to use this technology to reach conclusions about what people feel on the basis of their facial movements."[415]

Given the high-stakes contexts in which affect-recognition systems are being used and their rapid proliferation over the past several years, their scientific validity is an area in particular need of research and policy attention—especially when current scientific evidence suggests that claims being made about their efficacy don't hold up. In short, we need to scrutinize why entities are using faulty technology to make assessments about character on the basis of physical

appearance in the first place. This is particularly concerning in contexts such as employment, education, and criminal justice.

Face Datasets

Following the release of several studies, there continue to be significant performance disparities in commercial facial-recognition products across intersectional demographic subgroups.[416] In response, some companies are trying to "diversify" datasets to reduce bias. For instance, computer-vision company Clarifai revealed that it makes use of the profile photos from the dating website OkCupid to build large and "diverse" datasets of faces.[417] Clarifai claims the company gave them explicit permission and access to the data, so it remains unclear to what extent such data brokering constitutes a legal privacy violation disproportionately affecting people of color. IBM undertook a similar endeavor after being audited, releasing its "Diversity in Faces" study, which included an "inclusive" dataset of faces from a wide variety of Flickr users.[418] Although most of the users whose images were harvested had given permissions under an open Creative Commons license,[419] enabling widespread Internet use, none of the people in the photos gave IBM permission, again raising serious legal and ethical concerns about such practices.[420]

The problematic practice of scraping online images to produce diverse datasets is not limited to industry alone. Researchers Adam Harvey and Jules LaPlace exposed similar methods used to collect faces for academic datasets.[421] Most notably, the DUKE MTMC dataset,[422] Brainwash dataset,[423] and others[424] were collected by setting up surveillance cameras at college campuses, detecting and cropping out the faces of unsuspecting students to add to their database.

Ultimately, simply "diversifying the dataset" is far from sufficient to quell concerns about the use of facial-recognition technology. In fact, the face datasets themselves are a collection of artifacts to uncover, the assemblage of which reveals a set of decisions that were made regarding whom to include and whom to omit, but more importantly whom to exploit. It will be essential to continue to tell these stories, and to begin to uncover and perhaps challenge our accepted practices in the field, and the problematic patterns they reveal.[425]

2.6 Health

AI technologies today mediate people's experiences of health in many ways: from popular consumer-based technologies like Fitbits and the Apple Watch, to automated diagnostic support systems in hospitals, to the use of predictive analytics on social-media platforms to predict self-harming behaviors. AI also plays a role in how health insurance companies generate health-risk scores and in the ways government agencies and healthcare organizations allocate medical resources.[426]

Much of this activity comes with the aim of improving people's health and well-being through increased personalization of health, new forms of engagement, and clinical efficiency, popularly characterizing AI in health as an example of "AI for good" and an opportunity to tackle global health challenges.[427] This appeals to concerns about information complexities of biomedicine, population-based health needs, and the rising costs of healthcare. However, as AI technologies have rapidly moved from controlled lab environments into real-life health contexts, new social concerns are also fast emerging.

The Expanding Scale and Scope of Algorithmic Health Infrastructures

Advances in machine learning techniques and cloud-computing resources have made it possible to classify and analyze large amounts of medical data, allowing the automated and accurate detection of conditions like diabetic retinopathy and forms of skin cancer in medical settings.[428] At the same time, eager to apply AI techniques to health challenges, technology companies have been analyzing everyday experiences like going for a walk, food shopping, sleeping, and menstruating to make inferences and predictions about people's health behavior and status.[429]

While such developments may offer future positive health benefits, little empirical research has been published about how AI will impact patient health outcomes or experiences of care. Furthermore, the data- and cloud-computing resources required for training models to AI health systems have created troubling new opportunities, expanding what counts as "health data," but also the boundaries of healthcare. The scope and scale of these new "algorithmic health infrastructures"[430] give rise to a number of social, economic, and political concerns.

The proliferation of corporate-clinical alliances for sharing data to train AI models illustrates these infrastructural impacts. The resulting commercial incentives and conflicts of interest have made ethical and legal issues around health data front-page news. Most recently, a whistle-blower report alerted the public to serious privacy risks stemming from a partnership, known as Project Nightingale, between Google and Ascension,[431] one of the largest nonprofit health systems in the US. The report claimed that patient data transferred between Ascension and Google was not "de-identified."[432] Google helped migrate Ascension's infrastructure to their cloud environment, and in return received access to hundreds of thousands of privacy-protected patient medical records to use in developing AI solutions for Ascension and also to sell to other healthcare systems.[433]

Google, however, is not alone. Microsoft, IBM, Apple, Amazon, and Facebook, as well as a wide range of healthcare start-ups, have all made lucrative "data partnership" agreements with a wide range of healthcare organizations (including many university research hospitals and insurance companies) to gain access to health data for the training and development of AI-driven health systems.[434] Several of these have resulted in federal probes and lawsuits around improper use of patient data.[435]

However, even when current regulatory policies like HIPAA are strictly followed, security and privacy vulnerabilities can exist within larger technology infrastructures, presenting serious challenges for the safe collection and use of Electronic Health Record (EHR) data. New research shows that it is possible to accurately link two different de-identified EHR datasets using computational methods, so as to create a more complete history of a patient without using any personal health information of the patient in question.[436] Another recent research study showed that it is possible to create reconstructions of patients' faces using de-identified MRI images, which could then be identified using facial-recognition systems.[437] Similar concerns have prompted a lawsuit against the University of Chicago Medical Center and Google claiming that Google is "uniquely able to determine the identity of almost every medical record the university released" due to its expertise and resources in AI development.[438] The potential harm from misuse of these new health data capabilities is of grave concern, especially as AI health technologies continue to focus on predicting risks that could impact healthcare access or stigmatize individuals, such as recent attempts to diagnose complex behavioral health conditions like depression and schizophrenia from social-media data.[439]

New Social Challenges for the Healthcare Community

This year a number of reports, papers, and op-eds were published on AI ethics in healthcare.[440] Although mostly generated by physicians and medical ethicists in Europe and North America, these early efforts are important for better understanding the situated uses of AI systems in healthcare.

For example, the European and North American Radiology Societies recently issued a statement that outlines key ethical issues for the field, including algorithmic and automation bias in relation to medical imaging.[441] Radiology is currently one of the medical specialties where AI systems are the most advanced. The statement openly acknowledges how clinicians are reckoning with the increased value and potential harms around health data used for AI systems: "AI has noticeably altered our perception of radiology data—their value, how to use them, and how they may be misused."[442]

These challenges include possible social harms for patients, such as the potential for clinical decisions to be nudged or guided by AI systems in ways that don't (necessarily) bring people health benefits, but are in service to quality metric requirements or increased profit. Importantly, misuses also extend beyond the ethics of patient care to consider how AI technologies are reshaping medical organizations themselves (e.g., "radiologist and radiology departments will also *be* data" for healthcare administrators)[443] and the wider health domain by "blurring the line" between academic research and commercial AI uses of health data.[444]

Importantly, medical groups are also pushing back against the techno-solutionist promises of AI, crafting policy recommendations to address social concerns. For example, the Academy of Medical Royal Colleges (UK) 2019 report, "Artificial Intelligence in Healthcare," pragmatically

states: "Politicians and policymakers should avoid thinking that AI is going to solve all the problems the health and care systems across the UK are facing."[445] The American Medical Association has been working on an AI agenda for healthcare, too, also adopting the policy "Augmented Intelligence in Health Care"[446] as a framework for thinking about AI in relation to multiple stakeholder concerns, which include the needs of physicians, patients, and the broader healthcare community.

There have also been recent calls for setting a more engaged agenda around AI and health. This year Eric Topol, a physician and AI/ML researcher, questioned the promises of AI to fix systemic healthcare issues, like clinician burnout, without the collective action and involvement of healthcare workers.[447] Physician organizing is needed not because doctors should fear being replaced by AI, but to ensure that AI benefits people's experiences of care. "The potential of A.I. to restore the human dimension in health care," Topol argues, "will depend on doctors stepping up to make their voices heard."[448]

More voices are urgently needed at the table—including the expertise of patient groups, family caregivers, community health workers, and nurses—in order to better understand how AI technologies will impact diverse populations and health contexts. We have seen how overly narrow approaches to AI in health have resulted in systems that failed to account for darker skin tones in medical imaging data,[449] and cancer treatment recommendations that could lead to racially disparate outcomes due to training data from predominantly white patients.[450]

Importantly, algorithmic bias in health data cannot always be corrected by gathering more data, but requires understanding the social context of the health data that has already been collected. Recently, Optum's algorithm designed to identify "high-risk" patients in the US was based on the number of medical services a person used, but didn't account for the numerous socioeconomic reasons around the nonuse of needed health services, such as being underinsured or the inability to take time off from work.[451] With long histories of addressing such social complexities, research from fields like medical sociology and anthropology, nursing, human-computer interaction, and public health is needed to protect against the implementation of AI systems that (even when designed with good intentions) worsen health inequities.[452]

2.7 Advances in the Machine Learning Community

The Tough Road Toward Sociotechnical Perspectives

As research and perspectives on the social implications of AI evolve, machine learning (ML) research communities are realizing the limitations of narrow "fairness" definitions and are shifting their focus to more impactful interventions and strategies, as well as fostering an increased openness toward active inclusion and engagement with other disciplines.

In our 2018 AI Now Report, we critically assessed the affordances and limitations of technical fixes to problems of fairness.[453] Since then, several convincing critiques have emerged that further explain how these approaches fundamentally distract from more urgent issues,[454] abstract away societal context,[455] are incommensurate with the political reality of how data scientists approach "problem formulation,"[456] and fail to address the hierarchical logic that produces unlawful discrimination.[457]

Responding to these criticisms, many technical researchers have turned to the use of so-called "causal" or "counterfactual" fairness methods. Rather than relying on the correlations that most ML models use to make their predictions, these approaches aim to draw causal diagrams that explain how different types of data produce various outcomes. When analyzed for use of sensitive or protected categories, such as race or gender, these researchers seek to declare an ML "fair" if factors like race or gender do not causally influence the model's prediction.

While the intentions behind this work may be commendable, there are still clear limitations to these approaches, primarily in their ability to address historical disparities and ongoing structural injustices.[458] As Lily Hu explains in the context of racial health disparities, "Whatever [level of] health Black people *would have had* in some convoluted counterfactual scenario is frankly irrelevant to the question of whether actually existing inequality is a matter of injustice—let alone what can be done to remedy it."[459] In addition, the value of these assessments hinges on how to define which individual characteristics should or should not factor into the algorithm's final prediction.[460] Such decisions are often themselves politically, culturally, and socially influenced, and the power imbalance between those making such determinations and those impacted remains clear and unaddressed.[461]

Techniques for interpreting and explaining ML systems have also gained popularity. However, they suffer from many of these same critiques, and have been shown to be fundamentally fragile and prone to manipulation,[462] and to ignore a long history of insights from the social sciences.[463]

As a result, some researchers have begun to push harder on the need for interdisciplinary approaches,[464] and for integrating lessons from social sciences and humanities into the practice of developing AI systems.[465] Some practical strategies have emerged, including methods to document the development of machine learning models to enforce some level of additional ethical reflection and reporting throughout the engineering process.[466] Industry-led efforts by the Partnership on AI and IEEE are also attempting to consolidate these documentation proposals and to standardize reporting requirements across the industry.[467]

This year, more algorithmic audits also uncovered disproportionate performance or biases within AI systems ranging from self-driving-car software that performed differently for darker- and lighter-skinned pedestrians,[468] gender bias in online biographies,[469] skewed representations in object recognition from lower-income environments,[470] racial differences in algorithmic pricing,[471] and differential prioritization in healthcare,[472] as well as performance disparities in facial recognition.[473] In several cases, these audits had a tangible impact on improving the lives of

people unfairly affected.[474] They also had a substantial impact on policy discussions.[475] For instance, two audit studies of facial-recognition systems, including the widely recognized *Gender Shades*,[476] led to subsequent audit studies by the National Institute of Standards and Technology[477] and other researchers,[478] including the ACLU of Northern California's audits of Amazon Rekognition, which falsely matched 28 Congress members[479] and 27 mostly minority athletes to criminal mugshots.[480]

Confronting AI's Inherent Vulnerabilities

Concerns over the vulnerabilities of AI systems also gained greater attention this year, highlighting the urgent need for them to be subjected to the same scrutiny applied to automation technologies in other engineering fields, such as aviation and power systems.

Among the most urgent vulnerabilities to address is the danger of data-poisoning techniques, a method of exploitation in which a bad actor can fiddle with AI training data to alter a system's decisions. A classic example is spam filtering, where intentionally curating the content of messages that teach a spam filter how spam looks can help certain types of spam pass through the filter undetected.[481]

A second type of AI vulnerability that can be exploited is the so-called "back door," which lets attackers find ways to infiltrate an AI system through code that malicious programmers embed in systems they trained or designed for later infiltration by a bad actor. Researchers at NYU showed that back-door attacks may result in a model that has state-of-the-art performance on the user's training and validation samples (datasets used to test AI models), but behaves badly when confronted with specific attacker-chosen inputs.[482] The researchers used the back door to poison an AI road sign detector (commonly used in autonomous vehicles) into misclassifying US stop signs. And when they "retrained" the model to work on Swedish stop signs, the earlier poisoning effects carried over. This type of vulnerability raises serious concerns given the rapid move toward outsourcing the training procedures of ML models to cloud platforms.[483]

A related trend is the move to reduce training costs by repurposing and retraining AI models for new or specific tasks, a phenomenon called *transfer learning.* Transfer learning is particularly popular for applications that require large models, such as natural-language processing[484] or image classification.[485] Instead of starting from scratch, one retrains the parameters of a preexisting central model with more specific data for a new task or domain. Researchers show that this "centralization of model training increases their vulnerability to misclassification attacks," especially when such central models are publicly available.[486]

Adversarial attacks are particularly effective against systems with a high number of inputs, which are the variables that an AI model considers to make a decision or prediction when deployed.[487] This reliance on a large number of inputs is inherent to computer-vision systems, where typically each pixel is an input. It is likely also an issue for applications where automated decision systems

rely on a variety of inputs to make predictions about human behavior or preferences. Such models rely on diverse data sources, including social-network data, search entries, location tracking, energy use, and other revealing data about individual behavior and preferences. Such vulnerabilities expose people to misclassification, hacking, and strategic manipulation. Researchers from Harvard and MIT convincingly explained these concerns for the context of medical diagnostics.[488]

While research exposing technical vulnerabilities and proposing new defenses against them is now of high priority, building robust machine learning systems is still an elusive goal. A group of researchers across Google Brain, MIT, and the University of Tübingen recently surveyed the field and concluded that few defense mechanisms have succeeded. There is consensus in the field that most papers that propose defenses are quickly shown to be either incorrect or insufficient. The group observes that "[r]esearchers must be very careful to not deceive themselves unintentionally when performing evaluations."[489]

We must be extra careful when bringing AI systems to contexts where their errors lead to social harm. Similar to our discussion of fairness and bias in the 2018 AI Now report,[490] any debate about vulnerabilities should approach issues of power and hierarchy, looking at who is in a position to produce and profit from these systems, who determines how vulnerabilities are accounted for and addressed, and who is most likely to be harmed.

Despite the fact that social sciences and humanities approaches have a long history in information security and risk management,[491] research that addresses both social and technical dimensions in security is necessary, but still relatively nascent.[492] Central in this challenge is redrawing the boundaries of analysis and design to expand beyond the algorithm,[493] and securing channels for all affected stakeholders to democratically steer system development and to dissent when concerns arise.[494]

CONCLUSION

Despite the growth of ethical frameworks, AI systems continue to be deployed rapidly across domains of considerable social significance—in healthcare, education, employment, criminal justice, and many others—without appropriate safeguards or accountability structures in place. Many urgent concerns remain, and the agenda of issues to be addressed continues to grow: the environmental harms caused by AI systems are considerable, from extraction of materials from our earth to the extraction of labor from our communities. In healthcare, increasing dependence on AI systems will have life-or-death consequences. New research also highlights how AI systems are particularly prone to security vulnerabilities and how the companies building these systems are inciting fundamental changes to the landscape of our communities, resulting in geographic displacement.

Yet the movements of the past year give reason to hope, marked by a groundswell of pushback from both expected and unexpected places, from regulators and researchers to community organizers and activists to workers and advocates. Together, they are building new coalitions upon legacies of older ones, and forging new bonds of solidarity. If the past year has shown us anything, it is that our future will not be determined by the inevitable progress of AI, nor are we doomed to a dystopic future. The implications of AI will be determined by us—and there is much work ahead to ensure that the future looks bright.

ENDNOTES

1. See, for example, “Community Control over Police Surveillance,” ACLU, https://www.aclu.org/issues/privacy-technology/surveillance-technologies/community-control-over-police-surveillance; and Lee V. Gaines, “Illinois Doesn’t Track Electronic Monitoring Data, but New Legislation Would Require It,” Illinois Public Media, June 17, 2019, https://will.illinois.edu/news/story/illinois-doesnt-track-electronic-monitoring-data-but-new-legislation-would.

2. Dillon Reisman, Jason Schultz, Kate Crawford, and Meredith Whittaker, “Algorithmic Impact Assessments: A Practical Framework for Public Agency Accountability,” AI Now Institute, April 2018, https://ainowinstitute.org/aiareport2018.pdf.

3. Margaret Mitchell, Simone Wu, Andrew Zaldivar, Parker Barnes, Lucy Vasserman, Ben Hutchinson, Elena Spitzer, Inioluwa Deborah Raji, and Timnit Gebru, “Model Cards for Model Reporting,” Proceedings of the Conference on Fairness, Accountability, and Transparency, FAT* '19 (2019): 220–229, https://doi.org/10.1145/3287560.3287596.

4. Timnit Gebru, Jamie Morgenstern, Briana Vecchione, Jennifer Wortman Vaughan, Hanna Wallach, Hal Daumeé III, and Kate Crawford, "Datasheets for Datasets," *arXiv:1803.09010* (2018), https://arxiv.org/abs/1803.09010?context=cs.

5. For example, see Brent Hecht et al, “It’s Time to Do Something: Mitigating the Negative Impacts of Computing through a Change to the Peer Review Process,” ACM Future of Computing Blog, March 29, 2018, https://acm-fca.org/2018/03/29/negativeimpacts/.

6. Lisa Feldman Barrett et al., “Emotional Expressions Reconsidered: Challenges to Inferring Emotion From Human Facial Movements,” Psychological Science in the Public Interest 20, no.1 (2019): 1–68, https://journals.sagepub.com/stoken/default+domain/10.1177%2F1529100619832930-FREE/pdf.

7. See, for example, Alex Rosenblat, “When Your Boss Is an Algorithm,” *New York Times,* October 12, 2018, https://www.nytimes.com/2018/10/12/opinion/sunday/uber-driver-life.html; and Jeremias Adams-Prassl, “The Algorithmic Boss”, NYU Law, October 28, 2019, https://its.law.nyu.edu/eventcalendar/index.cfm?fuseaction=main.detail&id=73302.

8. Joshua Brustein, “Warehouses Are Tracking Workers’ Every Muscle Movement,” *Bloomberg,* November 5, 2019, https://www.bloomberg.com/news/articles/2019-11-05/am-i-being-tracked-at-work-plenty-of-warehouse-workers-are.

9. Colin Lecher, “How Amazon Automatically Tracks and Fires Warehouse Workers for ‘Productivity,’” *The Verge,* April 25, 2019, https://www.theverge.com/2019/4/25/18516004/amazon-warehouse-fulfillment-centers-productivity-firing-terminations.

10. Abdi Muse, Bhairavi Desai, Veena Dubal, and Meredith Whittaker, “Organizing Tech” panel at AI Now Symposium, October 2, 2019, https://ainowinstitute.org/symposia/videos/organizing-tech.html.

11. Daniel Flaming and Patrick Burns, Economic Roundtable, “Too Big to Govern: Public Balance Sheet for the World’s Largest Store,” November 2019, https://economicrt.org/wp-content/uploads/2019/11/Too-Big-to-Govern.pdf.

12. Chris Ramsaroop, "Reality Check 101: Rethinking the Impact of Automation and Surveillance on Farm Workers," *Data & Society: Points*, September 6, 2019, https://points.datasociety.net/reality-check-101-c6e501c3b9a3.

13. Juliana Feliciano Reyes, "Hotel Housekeeping on Demand: Marriott Cleaners Say This App Makes Their Job Harder," *Philadelphia Inquirer*, July 2, 2018, https://www.inquirer.com/philly/news/hotel-housekeepers-schedules-app-marriott-union-hotsos-20180702.html.

14. Juliana Feliciano Reyes, "In the Basement of CHOP, Warehouse Workers Say They're Held to Impossible Quotas," *Philadelphia Inquirer,* April 22, 2019, https://www.inquirer.com/news/warehouse-workers-quotas-rate-childrens-hospital-of-philadelphia-canon-20190422.html.

15. Rose Eveleth, "Your Employer May Be Spying on You—and Wasting Its Time," *Scientific American,* August 16, 2019, https://www.scientificamerican.com/article/your-employer-may-be-spying-on-you-and-wasting-its-time/.

16. A substantial number of firms adopting this strategy are funded by the same investor: the Japanese firm Softbank. See Nathaniel Popper, Vindu Goel, and Arjun Harindranath, "The SoftBank Effect: How $100 Billion Left Workers in a Hole," *New York Times*, November 12, 2019, https://www.nytimes.com/2019/11/12/technology/softbank-startups.html.

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

18. See Jaden Urbi, "Some Transgender Drivers Are Being Kicked Off Uber's App," CNBC, August 8, 2018, https://www.cnbc.com/2018/08/08/transgender-uber-driver-suspended-tech-oversight-facial-recognition.html; and Rob Hayes, "Uber, Lyft Drivers Rally in Downtown Los Angeles to Demand Better Wages, Employment Rights," Eyewitness News / ABC7, https://abc7.com/business/uber-lyft-drivers-rally-in-la-to-demand-better-wages-employment-rights/5353986/.

19. Vanessa Bain, "Dear Instacart Customers," October 9, 2019, https://medium.com/@vanessabain/dear-instacart-customers-664dbb59016e; Megan Rose Dickey, "Instacart Is under Fire for How It Compensates Shoppers," *TechCrunch,* November 12, 2019, https://techcrunch.com/2019/11/12/instacart-is-under-fire-for-how-it-compensates-shoppers/.

20. April Glaser, "How DoorDash, Postmates, and Other Delivery Services Tip Workers," *Slate,* July 23, 2019, https://slate.com/technology/2019/07/doordash-postmates-grubhub-instacart-tip-policies.html.

21. Sean Captain, "Instacart Delivery Drivers Say Tips Are Mysteriously Decreasing," *Fast Company,* October 9, 2019, https://www.fastcompany.com/90413156/tips-for-instacart-delivery-drivers-are-mysteriously-decreasing.

22. Faiz Siddiqui, "Uber and Lyft Slashed Wages. Now California Drivers Are Protesting Their IPOs," *Washington Post*, March 26, 2019, https://www.washingtonpost.com/technology/2019/03/26/uber-lyft-slashed-wages-now-california-drivers-are-protesting-their-ipos/.

23. Veena Dubal, "The Drive to Precarity: A Political History of Work, Regulation, & Labor Advocacy in San Francisco's Taxi & Uber Economies," *Berkeley Journal of Employment and Labor Law* 38, no. 1, February 21, 2017; UC Hastings Research Paper no. 236. Available at SSRN: https://ssrn.com/abstract=2921486.

24. Jim Stanford, "Bring Your Own Equipment and Wait for Work: Working for Uber Is a Lot Like Being a Dock Worker a Century Ago," *Star,* November 17, 2019,

https://www.thestar.com/business/opinion/2019/11/17/bring-your-own-equipment-and-wait-for-work-working-for-uber-is-a-lot-like-being-a-dock-worker-a-century-ago.html.

25. Noopur Raval, "Developing a Framework for Postcolonial Digital Labor," unpublished manuscript, 2017, https://www.academia.edu/35413303/Developing_a_framework_for_postcolonial_digital_labor.

26. Aditi Surie and Jyothi Koduganti, "The Emerging Nature of Work in Platform Economy Companies in Bengaluru, India: The Case of Uber and Ola Cab Drivers," *E-Journal of International and Comparative Labour Studies* 5, no. 3 (September–October 2016), http://ejcls.adapt.it/index.php/ejcls_adapt/article/view/224/.

27. Kristy "spamgirl" Milland, "The Unsupported Crowd: Exclusion of Indian Workers in Amazon Mechanical Turk Communities," 2017, http://kristymilland.com/papers/Milland.2017.The.Unsupported.Crowd.pdf.

28. Noopur Raval and Joyojeet Pal, "Making a 'Pro': 'Professionalism' after Platforms in Beauty-work," *Journal Proceedings of the ACM on Human-Computer Interaction* 3, no. CSCW (November 2019), https://dl.acm.org/citation.cfm?id=3359277.

29. Mark Graham and Mohammed Amir Anwar, "The Global Gig Economy: Towards a Planetary Labour Market?," *First Monday* 24, no. 4 (April 1, 2019), https://firstmonday.org/ojs/index.php/fm/article/view/9913/7748#p2.

30. Miranda Bogen and Aaron Rieke, "Help Wanted: An Examination of Hiring Algorithms, Equity, and Bias," *Upturn*, December 2018, https://www.upturn.org/static/reports/2018/hiring-algorithms/files/Upturn%20--%20Help%20Wanted%20-%20An%20Exploration%20of%20Hiring%20Algorithms,%20Equity%20and%20Bias.pdf.

31. Robert Booth, "Unilever Saves on Recruiters by Using AI to Assess Job Interviews," *Guardian*, October 25, 2019, https://www.theguardian.com/technology/2019/oct/25/unilever-saves-on-recruiters-by-using-ai-to-assess-job-interviews.

32. Rosalind S. Helderman, "HireVue's AI Face-Scanning Algorithm Increasingly Decides Whether You Deserve the Job," *Washington Post*, October 22, 2019, https://www.washingtonpost.com/technology/2019/10/22/ai-hiring-face-scanning-algorithm-increasingly-decides-whether-you-deserve-job/.

33. Daniel Greene and Ifeoma Ajunwa, "Automated Hiring Platforms as Technological Intermediaries and Brokers," Dan Greene, 2017, http://dmgreene.net/wp-content/uploads/2014/11/GreeneAjunwaAutomated-Hiring-Plaforms-as-Technological-Intermediaries-and-Brokers.pdf.

34. Bogen and Rieke, "Help Wanted: An Examination of Hiring Algorithms, Equity, and Bias," *Upturn*, December 2018, https://www.upturn.org/static/reports/2018/hiring-algorithms/files/Upturn%20--%20Help%20Wanted%20-%20An%20Exploration%20of%20Hiring%20Algorithms,%20Equity%20and%20Bias.pdf.

35. See Jim Fruchterman and Joan Mellea, "Expanding Employment Success for People with Disabilities," Benetech, November 2018, https://benetech.org/about/resources/expanding-employment-success-for-people-with-disabilities/; https://arxiv.org/pdf/1910.06144.pdf; https://ainowinstitute.org/discriminatingsystems.pdf.

36. Pauline Kim, "Data-Driven Discrimination at Work," William & Mary Law Review 48 (2017): 857–936, https://ssrn.com/abstract=2801251.

37. Rashida Richardson, Jason M. Schultz, and Vincent M. Southerland, "Litigating Algorithms," AI Now Institute, September 2019, https://ainowinstitute.org/litigatingalgorithms-2019-us.pdf.

38. Illinois General Assembly, Public Act 101-0260, http://www.ilga.gov/legislation/publicacts/fulltext.asp?Name=101-0260.

39. Manish Raghavan, Solon Barocas, Jon Kleinberg, and Karen Levy, "Mitigating Bias in Algorithmic Hiring: Evaluating Claims and Practices," June 21, 2019, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3408010.

40. Drew Harwell, "Rights Group Files Federal Complaint against AI-hiring Firm Citing Unfair, Deceptive Practices," *Washington Post,* November 6, 2019, https://www.washingtonpost.com/technology/2019/11/06/prominent-rights-group-files-federal-complaint-against-ai-hiring-firm-hirevue-citing-unfair-deceptive-practices/.

41. Pymetrics, "Pymetrics End User Agreement," https://www.pymetrics.com/terms-of-service/.

42. Ifeoma Ajunwa and Daniel Greene, "Platforms at Work: Automated Hiring Platforms and Other New Intermediaries in the Organization of Work," in *Work and Labor in the Digital Age,* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3248675.

43. See, for example, Ifeoma Ajunwa, Kate Crawford, and Jason Schultz, "Limitless Worker Surveillance," 105 Cal. Rev. 735, March 10, 2016, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2746211; Ifeoma Ajunwa, "Algorithms at Work: Productivity Monitoring Applications and Wearable Technology as the New Data-Centric Research Agenda for Employment and Labor Law," *63 St. Louis U.L.J,* September 10, 2018, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3247286; and Meredith Whittaker et al., "Disability, Bias, and AI," AI Now Institute, November 2019, https://ainowinstitute.org/disabilitybiasai-2019.pdf.

44. There are many sources of automation. For the purposes of this report, we adopt a broad definition of automation that goes beyond technical AI sources.

45. Kweilin Ellingrud, "The Upside of Automation: New Jobs, Increased Productivity and Changing Roles for Workers," *Forbes,* October 23, 2019, https://www.forbes.com/sites/kweilinellingrud/2018/10/23/the-upside-of-automation-new-jobs-increased-productivity-and-changing-roles-for-workers/#9bae2fb7df04.

46. Carl Benedikt Frey and Michael A. Osborne, "The Future of Employment: How Susceptible Are Jobs to Computerisation?" Oxford Martin, September 17, 2013, https://www.oxfordmartin.ox.ac.uk/downloads/academic/The_Future_of_Employment.pdf.

47. See Mark Muro, Robert Maxim, and Jacob Whiton, "Automation and Artificial Intelligence: How Machines Are Affecting People and Places," Brookings Institution (January 2019), https://www.brookings.edu/wp-content/uploads/2019/01/2019.01_BrookingsMetro_Automation-AI_Report_Muro-Maxim-Whiton-FINAL-version.pdf; and "Artificial Intelligence, Automation, and the Economy," Executive Office of the President (December 2016): 14, https://obamawhitehouse.archives.gov/sites/whitehouse.gov/files/documents/Artificial-Intelligence-Automation-Economy.PDF.

48. Brookings employed a backward- and forward-looking analysis of the impacts of automation from 1980 to 2016 and 2016 to 2030 across approximately 800 occupations. See Muro et al., "Automation and Artificial Intelligence," 33, https://www.brookings.edu/wp-content/uploads/2019/01/2019.01_BrookingsMetro_Automation-AI_Report_Muro-Maxim-Whiton-FINAL-version.pdf.

49. Muro et al., "Automation and Artificial Intelligence," 33–34, https://www.brookings.edu/wp-content/uploads/2019/01/2019.01_BrookingsMetro_Automation-AI_Report_Muro-Maxim-Whiton-FINAL-version.pdf.

50. Muro et al., "Automation and Artificial Intelligence," 45–46, https://www.brookings.edu/wp-content/uploads/2019/01/2019.01_BrookingsMetro_Automation-AI_Report_Muro-Maxim-Whiton-FINAL-version.pdf.

51. Muro et al., "Automation and Artificial Intelligence," 7, https://www.brookings.edu/wp-content/uploads/2019/01/2019.01_BrookingsMetro_Automation-AI_Report_Muro-Maxim-Whiton-FINAL-version.pdf.

52. Kelemwork Cook, Duwain Pinder, Shelley Stewart III, Amaka Uchegbu, and Jason Wright, "The Future of Work in Black America," McKinsey & Company, October 2019, https://www.mckinsey.com/featured-insights/future-of-work/the-future-of-work-in-black-america.

53. Susan Lund, James Manyika, et al., "The Future of Work in America: People and Places, Today and Tomorrow," McKinsey Global Institute (July 2019): 61, https://www.mckinsey.com/~/media/McKinsey/Featured%20Insights/Future%20of%20Organizations/The%20future%20of%20work%20in%20America%20People%20and%20places%20today%20and%20tomorrow/MGI-The-Future-of-Work-in-America-Report-July-2019.ashx.

54. Lund, Manyika, et al, "The Future of Work in America," https://www.mckinsey.com/~/media/McKinsey/Featured%20Insights/Future%20of%20Organizations/The%20future%20of%20work%20in%20America%20People%20and%20places%20today%20and%20tomorrow/MGI-The-Future-of-Work-in-America-Report-July-2019.ashx.

55. Lund, Manyika, et al, "The Future of Work in America," 13, https://www.mckinsey.com/~/media/McKinsey/Featured%20Insights/Future%20of%20Organizations/The%20future%20of%20work%20in%20America%20People%20and%20places%20today%20and%20tomorrow/MGI-The-Future-of-Work-in-America-Report-July-2019.ashx.

56. Erin Winick, "Every Study We Could Find on What Automation Will Do To Jobs in One Chart," *MIT Technology Review,* January 25, 2018, https://www.technologyreview.com/s/610005/every-study-we-could-find-on-what-automation-will-do-to-jobs-in-one-chart/.

57. Winick, "Every Study We Could Find on What Automation Will Do To Jobs in One Chart," https://www.technologyreview.com/s/610005/every-study-we-could-find-on-what-automation-will-do-to-jobs-in-one-chart/.

58. Sarah Myers West, Meredith Whittaker, and Kate Crawford, "Discriminating Systems: Gender, Race, and Power in AI," AI Now Institute, April 2019, https://ainowinstitute.org/discriminatingsystems.pdf.

59. Şerife Wong, "Fluxus Landscape: An Expansive View of AI Ethics and Governance," *Kumu*, August 20, 2019, https://icarus..kumu.io/fluxus-landscape; Jessica Fjeld et al., "Principled Artificial Intelligence: A Map of Ethical and Rights-Based Approaches," Berkman Klein Center for Internet & Society at Harvard University, July 4, 2019, https://ai-hr.cyber.harvard.edu/primp-viz.html; Luciano Floridi and Josh Cowls, "A Unified Framework of Five Principles for AI in Society," *Harvard Data Science Review*, June 22, 2019, https://doi.org/10.1162/99608f92.8cd550d1; Thilo Hagendorff, "The Ethics of AI Ethics—An Evaluation of Guidelines," *arXiv:1903.03425 [Cs, Stat]*, October 11, 2019, http://arxiv.org/abs/1903.03425; Yi Zeng, Enmeng Lu, and Cunqing Huangfu, "Linking Artificial Intelligence Principles," *arXiv:1812.04814 [Cs]*, December 12, 2018, http://arxiv.org/abs/1812.04814; Anna Jobin, Marcello Ienca, and Effy Vayena, "The Global Landscape of AI Ethics Guidelines," *Nature Machine Intelligence* 1, no. 9 (September 2019): 389–99, https://doi.org/10.1038/s42256-019-0088-2.

60. "Our Approach: Microsoft AI Principles," Microsoft, https://www.microsoft.com/en-us/ai/our-approach-to-ai; "IBM'S Principles for Data Trust and Transparency," THINKPolicy, May 30, 2018, https://www.ibm.com/blogs/policy/trust-principles/; "Our Principles," Google AI, accessed November 20, 2019, https://ai.google/principles/.

61. "Official Launch of the Montréal Declaration for Responsible Development of Artificial Intelligence," Mila, December 4, 2018, https://mila.quebec/en/2018/12/official-launch-of-the-montreal-declaration-for-responsible-development-of-artificial-intelligence/; Access Now Policy Team, "The Toronto Declaration: Protecting the Rights to Equality and Non-Discrimination in Machine Learning Systems," Access Now (blog), May 16, 2018, https://www.accessnow.org/the-toronto-declaration-protecting-the-rights-to-equality-and-non-discrimination-in-machine-learning-systems/.

62. "OECD Principles on Artificial Intelligence," Organisation for Economic Co-Operation and Development, accessed November 20, 2019, https://www.oecd.org/going-digital/ai/principles/.

63. "OpenAI Charter," OpenAI, accessed November 20, 2019, https://openai.com/charter/; "Tenets," Partnership on AI, accessed November 20, 2019, https://www.partnershiponai.org/tenets/.

64. See Vidushi Marda, "Introduction" in APC, Article 19, and SIDA, "Artificial Intelligence: Human Rights, Social Justice and Development," Global Information Watch 2019, November 2019, https://giswatch.org/sites/default/files/gisw2019_artificial_intelligence.pdf.

65. Daniel Greene, Anna Lauren Hoffmann, and Luke Stark, "Better, Nicer, Clearer, Fairer: A Critical Assessment of the Movement for Ethical Artificial Intelligence and Machine Learning," January 8, 2019, https://doi.org/10.24251/HICSS.2019.258; Daniel Greene et al., "A Critical Assessment of the Movement for Ethical Artificial Intelligence and Machine Learning," accessed November 20, 2019, http://dmgreene.net/wp-content/uploads/2018/12/Greene-Hoffmann-Stark-Better-Nicer-Clearer-Fairer-HICSS-Final-Submission-Revised.pdf; Jess Whittlestone et al., "The Role and Limits of Principles in AI Ethics: Towards a Focus on Tensions," n.d., 7; Roel Dobbe and Morgan Ames, "Up Next For FAT*: From Ethical Values To Ethical Practices," Medium, February 9, 2019, https://medium.com/@roeldobbe/up-next-for-fat-from-ethical-values-to-ethical-practices-ebbed9f6adee.

66. Brent Mittelstadt, "Principles Alone Cannot Guarantee Ethical AI," *Nature Machine Intelligence* 1 (November 2019): 501–507, https://dx.doi.org/10.2139/ssrn.3391293.

67. Olivia Solon, "Microsoft Funded Firm Doing Secret Israeli Surveillance on West Bank," NBC News, October 28, 2019, https://www.nbcnews.com/news/all/why-did-microsoft-fund-israeli-firm-surveils-west-bank-palestinians-n1072116.

68. Human Rights Watch, "Israel and Palestine: Events of 2018," accessed November 21, 2019, https://www.hrw.org/world-report/2019/country-chapters/israel/palestine#1b36d4.

69. Evan Selinger and Woodrow Hartzog, "What Happens When Employers Can Read Your Facial Expressions?," *New York Times*, October 17, 2019, https://www.nytimes.com/2019/10/17/opinion/facial-recognition-ban.html.

70. Rich Sauer, "Six Principles to Guide Microsoft's Facial Recognition Work," Microsoft on the Issues, December 17, 2018, https://blogs.microsoft.com/on-the-issues/2018/12/17/six-principles-to-guide-microsofts-facial-recognition-work/.

71. Olivia Solon, "MSFT Hires Eric Holder to Audit AnyVision's Facial Recognition Tech," CNBC, November 15, 2019,
https://www.cnbc.com/2019/11/15/msft-hires-eric-holder-to-audit-anyvisions-facial-recognition-tech.html.

72. Sundar Pichai, "AI at Google: Our Principles," Google, June 7, 2018,
https://blog.google/technology/ai/ai-principles/.

73. Googlers Against Transphobia, "Googlers Against Transphobia and Hate," Medium, April 1, 2019,
https://medium.com/@against.transphobia/googlers-against-transphobia-and-hate-b1b0a5dbf76.

74. Nick Statt, "Google Dissolves AI Ethics Board Just One Week after Forming It," *The Verge*, April 4, 2019,
https://www.theverge.com/2019/4/4/18296113/google-ai-ethics-board-ends-controversy-kay-coles-james-heritage-foundation.

75. See Tracy Jan and Elizabeth Dwoskin, "HUD Is Reviewing Twitter's and Google's Ad Practices as Part of Housing Discrimination Probe," *Washington Post*, March 28, 2019,
https://www.washingtonpost.com/business/2019/03/28/hud-charges-facebook-with-housing-discrimination/; Julia Angwin, Ariana Tobin and Madeleine Varner, "Facebook (Still) Letting Housing Advertisers Exclude Users by Race," *ProPublica*, November 21, 2017,
https://www.propublica.org/article/facebook-advertising-discrimination-housing-race-sex-national-origin; and Muhammad Ali et al., "Discrimination through Optimization: How Facebook's Ad Delivery Can Lead to Skewed Outcomes," *arXiv:1904.02095v5 [cs.CY]*, September 12, 2019, https://arxiv.org/pdf/1904.02095.pdf.

76. Article 19, "Governance with Teeth: How Human Rights Can Strengthen FAT and Ethics Initiatives on Artificial Intelligence, April 2019,
https://www.article19.org/wp-content/uploads/2019/04/Governance-with-teeth_A19_April_2019.pdf.

77. See Filippo Raso et al., "Artificial Intelligence & Human Rights: Opportunities & Risks," Berkman Klein Center for Internet & Society, September 25, 2018, http://nrs.harvard.edu/urn-3:HUL.InstRepos:38021439; Philip Alston, "Report of the Special Rapporteur on Extreme Poverty and Human Rights," October 11, 2019,
https://srpovertyorg.files.wordpress.com/2019/10/a_74_48037_advanceuneditedversion-1.pdf; and Jason Pielemeier, "The Advantages and Limitations of Applying the International Human Rights Framework to Artificial Intelligence," *Data & Society: Points*, June 6, 2018,
https://points.datasociety.net/the-advantages-and-limitations-of-applying-the-international-human-rights-framework-to-artificial-291a2dfe1d8a.

78. For China rights violations, see Marco Rubio, "We Must Stand Up to China's Abuse of Its Muslim Minorities," *Guardian*, October 31, 2019,
https://www.theguardian.com/commentisfree/2019/oct/31/china-uighurs-muslims-religious-minorities-marco-rubio; for US rights violations, see "UN Rights Chief 'Appalled' by US Border Detention Conditions, Says Holding Migrant Children May Violate International Law," *UN News*, July 8, 2019,
https://news.un.org/en/story/2019/07/1041991.

79. Jacob Metcalf, Emanuel Moss, and danah boyd, "Owning Ethics: Corporate Logics, Silicon Valley, and the Institutionalization of Ethics," *Data & Society,* September 10, 2019,
https://datasociety.net/output/owning-ethics-corporate-logics-silicon-valley-and-the-institutionalization-of-ethics/.

80. Paul Karoff, "Embedding Ethics in Computer Science Curriculum," *Harvard Gazette*, January, 25, 2019,
https://news.harvard.edu/gazette/story/2019/01/harvard-works-to-embed-ethics-in-computer-science-curriculum/. See also Greg Epstein, "Teaching Ethics in Computer Science the Right Way with Georgia Tech's Charles Isbell," *TechCrunch*, September 5, 2019,
https://techcrunch.com/2019/09/05/teaching-ethics-in-computer-science-the-right-way-with-georgia-techs-charles-isbell/; Zeninjor Enwemeka, "Solving the Tech Industry's Ethics Problem Could Start In The Classroom," National Public Radio, May 31, 2019,

https://www.npr.org/2019/05/31/727945689/solving-the-tech-industrys-ethics-problem-could-start-in-the-classroom; and Jenny Anderson, "MIT Developed a Course to Teach Tweens about the Ethics of AI," *Quartz,* September 4, 2019,
https://qz.com/1700325/mit-developed-a-course-to-teach-tweens-about-the-ethics-of-ai/.

81. Design Justice Network Principles, accessed November 24, 2019,
https://designjustice.org/read-the-principles.

82. Matt McFarland, "Feds Blame Distracted Test Driver in Uber Self-Driving Car Death," *CNN Business*, November 19, 2019, https://www.cnn.com/2019/11/19/tech/uber-crash-ntsb/index.html.

83. Kristen Lee, "Uber's Self-Driving Cars Made It Through 37 Crashes Before Killing Someone," *Jalopnik*, November 6, 2019,
https://jalopnik.com/ubers-self-driving-cars-made-it-through-37-crashes-befo-1839660767.

84. Kate Conger and Cade Metz, "Tech Workers Now Want to Know: What Are We Building This For?," *New York Times,* October 7, 2018,
https://www.nytimes.com/2018/10/07/technology/tech-workers-ask-censorship-surveillance.html.

85. Ryan Gallagher, "Google Shut Out Privacy and Security Teams from Secret China Project," *The Intercept*, November 29, 2018, https://theintercept.com/2018/11/29/google-china-censored-search/.

86. Erin McElroy, "Data, Dispossession, and Facebook: Toponymy and Techno-Imperialism in Gentrifying San Francisco," *Urban Geography* 40 no. 6 (2019): 826–845,
https://doi.org/10.1080/02723638.2019.1591143.

87. William Magnuson, "Why We Should be Worried about Artificial Intelligence on Wall Street," *Los Angeles Times*, November 1, 2019,
https://www.latimes.com/opinion/story/2019-11-01/artificial-intelligence-ai-wall-street.

88. Paula Chakravartty and Denise Ferreira da Silva, "Accumulation, Dispossession, and Debt: The Racial Logic of Global Capitalism—An Introduction," *American Quarterly* 64, no. 3 (September 2012): 361–385.

89. Desiree Fields, "Automated Landlord: Digital Technologies and Post-crisis Financial Accumulation," *Environment and Planning A: Economy and Space*, May 2019, https://doi.org/10.1177/0308518X19846514.

90. Erin McElroy, "Disruption at the Doorstep," *Urban Omnibus,* November 2019,
https://urbanomnibus.net/2019/11/disruption-at-the-doorstep/.

91. Agustín Cócola Gant, "Holiday Rentals: The New Gentrification Battlefront," *Sociological Research Online* 21, no. 3 (2016): 1–9.

92. Anti-Eviction Mapping Project, "Precarious Housing: Loss of SRO Hotels in Oakland," 2017,
http://arcg.is/nymnW.

93. Manissa M. Maharawal and Erin McElroy. "The Anti-Eviction Mapping Project: Counter Mapping and Oral History Toward Bay Area Housing Justice." *Annals of the American Association of Geographers* 108, no. 2 (2018): 380–389.

94. "State of Emergency: Special Report on California's Criminalization of Growing Homeless Encampments," *Democracy Now*, October 25, 2019,
https://www.democracynow.org/2019/10/25/state_of_emergency_special_report_on.

95. Anti-Eviction Mapping Project, "Rent Control for All," 2018, https://arcg.is/15X5bP.

96. Erin McElroy, "Digital Nomads in Siliconising Cluj: Material and Allegorical Double Dispossession," *Urban Studies*, July 2, 2019, https://doi.org/10.1177/0042098019847448.

97. Enikő Vincze and George Iulian Zamfir, "Racialized Housing Unevenness in Cluj-Napoca Under Capitalist Redevelopment," *City*, November 6, 2019, https://doi.org/10.1080/13604813.2019.1684078.

98. Ramona Giwargis, "Who is Behind the Anti-Google Protests?" *San Jose Spotlight*, January 9, 2019, https://sanjosespotlight.com/who-is-behind-the-anti-google-protests.

99. Victoria Turk, "How a Berlin Neighbourhood Took On Google and Won," *Wired*, October 26, 2018, https://www.wired.co.uk/article/google-campus-berlin-protests.

100. Lara Zarum, "#BlockSidewalk's War Against Google in Canada," *The Nation*, October 26, 2019, https://www.thenation.com/article/google-toronto-sidewalk-gentrification/.

101. Josh O'Kane, "Opponents of Sidewalk Labs Get Advice from German Tech Protestors," *Globe and Mail,* November 24, 2019, https://www.theglobeandmail.com/business/article-opponents-of-sidewalk-labs-get-advice-from-german-tech-protesters.

102. Jon Fingas, "San Francisco Bans City Use of Facial Recognition," *Engadget,* May 14, 2019, https://www.engadget.com/2019/05/14/san-francisco-bans-city-use-of-facial-recognition/.

103. Christine Fisher, "Oakland Bans City Use of Facial Recognition Software," *Engadget,* July 17, 2019, https://www.engadget.com/2019/07/17/oakland-california-facial-recognition-ban/.

104. Caroline Haskins, "A Second U.S. City Has Banned Facial Recognition," *Motherboard,* June 27, 2019, https://www.vice.com/en_us/article/paj4ek/somerville-becomes-the-second-us-city-to-ban-facial-recognition.

105. Colin Harris, "Montreal Grapples with Privacy Concerns as More Canadian Police Forces Use Facial Recognition," CBC, August 8, 2019, https://www.cbc.ca/news/canada/montreal/facial-recognition-artificial-intelligence-montreal-privacy-police-law-enforcement-1.5239892.

106. Allie Gross, "Detroiters Concerned over Facial Recognition Technology as Police Commissioners Table Vote," *Detroit Free Press,* June 27, 2019, https://www.freep.com/story/news/local/michigan/detroit/2019/06/27/detroiters-concerned-over-facial-recognition-technology/1567113001/.

107. See Ginia Bellafante, "The Landlord Wants Facial Recognition in Its Rent-Stabilized Buildings. Why?," *New York Times,* March 28, 2019, https://www.nytimes.com/2019/03/28/nyregion/rent-stabilized-buildings-facial-recognition.html; and Erin Durkin (@erinmdurkin), "The landlord of Brooklyn's Atlantic Plaza Towers has dropped his application to install facial recognition technology," Twitter, November 21, 2019, 12:45 p.m., https://twitter.com/erinmdurkin/status/1197571728173604864.

108. Stop LAPD Spying Coalition, accessed November 24, 2019, https://stoplapdspying.org/.

109. See City News Service, "LAPD Chief to Outline New Data Policies," NBC Los Angeles, April 9, 2019, https://www.nbclosangeles.com/news/local/LAPD-Chief-to-Outline-New-Data-Policies-508308931.html; and Stop LAPD Spying Coalition, "The People's Response to OIG Audit of Data-Driven Policing," Stop LAPD Spying, March 2019, https://stoplapdspying.org/wp-content/uploads/2019/03/Peoples_Response_with-hyper-links.pdf.

110. Stop LAPD Spying, Medium, April 4, 2019, https://medium.com/@stoplapdspying/on-tuesday-april-2nd-2019-twenty-eight-professors-and-forty-graduate-students-of-university-of-8ed7da1a8655.

111. Kristian Lum and William Isaac, "To predict and serve?" *Significance* 13, no. 5 (October 2016): 14–19, https://doi.org/10.1111/j.1740-9713.2016.00960.x,

112. Aila Slisco, "Protesters Denounce 'Spy Plane' Plan to Monitor St. Louis," *Newsweek,* October 10, 2019, https://www.newsweek.com/protesters-denounce-spy-plane-plan-monitor-st-louis-1464535.

113. Nellie Bowles, "Silicon Valley Came to Kansas Schools. That Started a Rebellion," *New York Times,* April 21, 2019, https://www.nytimes.com/2019/04/21/technology/silicon-valley-kansas-schools.html.

114. Media Justice, accessed November 24, 2019, https://mediajustice.org/

115. Tech Workers Coalition, accessed November 24, 2019, https://techworkerscoalition.org/.

116. "Take Back Tech: A People's Summit for a Surveillance Free Future," accessed November 24, 2019, https://mijente.net/takebacktech/#1566321457689-a14ae857-a59f.

117. Mijente, "The War against Immigrants: Trump's Tech Tools Powered by Palantir," August 2019, https://mijente.net/wp-content/uploads/2019/08/Mijente-The-War-Against-Immigrants_-Trumps-Tech-Tools-Powered-by-Palantir_.pdf.

118. Mijente, "Take Back Tech", #NoTechFor Ice, accessed November 19, 2019, https://notechforice.com/.

119. Rosalie Chan, "Protesters Blocked Palantir's Cafeteria to Pressure the $20 Billion Big Data Company to Drop Its Contracts with ICE," *Business Insider,* August 16, 2019, https://www.businessinsider.com/palantir-protest-palo-alto-activists-ice-contracts-2019-8.

120. Never Again Action, accessed November 24, 2019, https://www.neveragainaction.com/.

121. Jews for Racial and Economic Justice, accessed November 24, 2019, https://jfrej.org/.

122. Michael Grothaus, "Dozens of People Have Been Arrested at a #JewsAgainstICE Protest at NYC Amazon Books Store," *Fast Company*, August 12, 2019, https://www.fastcompany.com/90388865/dozens-of-people-have-been-arrested-at-a-jewsagainstice-protest-at-nyc-amazon-books-store.

123. Make the Road New York, accessed November 24, 2019, https://maketheroadny.org/.

124. Rachel Frazin, "Advocates Start Petition Asking Tech Conference to Drop Palantir as Sponsor over ICE Contracts," *The Hill*, October 23, 2019, https://thehill.com/policy/technology/467204-advocates-start-petition-asking-tech-conference-to-drop-palantir-as-sponsor.

125. Lizette Chapman, "Palantir Dropped by Berkeley Privacy Conference After Complaints," *Bloomberg,* June 5, 2019, https://www.bloomberg.com/news/articles/2019-06-05/palantir-dropped-by-berkeley-privacy-conference-after-complaints.

126. Rob Price and Rosalie Chan, "LGBTQ Tech Group Lesbians Who Tech Ditches Palantir as a Conference Sponsor over Human-Rights Concerns," *Business Insider,* August 26, 2019, https://www.businessinsider.com/lesbians-who-tech-ends-sponsorship-deal-palantir-human-rights-2019-8.

127. Shirin Gaffary, "The World's Biggest Women's Tech Conference Just Dropped Palantir as a Sponsor," *Recode,* August 28, 2019,

https://www.vox.com/recode/2019/8/28/20837365/anita-b-grace-hopper-palantir-sponsor-worlds-biggest-womens-tech-conference-dropped.

128. Athena, accessed November 27, 2019, https://athenaforall.org/.

129. Jimmy Tobias, "The Amazon Deal Was Not Brought Down by a Handful of Politicians: It Was Felled by a Robust Grassroots Coalition," *The Nation,* February 19, 2019, https://www.thenation.com/article/the-amazon-deal-was-not-brought-down-by-a-handful-of-politicians/.

130. David Streitfeld, "Activists Build a Grass-Roots Alliance Against Amazon," *New York Times,* November 26, 2019, https://www.nytimes.com/2019/11/26/technology/amazon-grass-roots-activists.html.

131. See Os Keyes, "The Bones We Leave Behind," *Real Life Magazine,* October 7, 2019, https://reallifemag.com/the-bones-we-leave-behind/; Georgetown Law Center on Privacy and Technology, "The Color of Surveillance," 2019, https://www.law.georgetown.edu/privacy-technology-center/events/color-of-surveillance-2019/; and Ed Pilkington, "Digital Dystopia: How Algorithms Punish the Poor," *Guardian,* October 14, 2019, https://www.theguardian.com/technology/2019/oct/14/automating-poverty-algorithms-punish-poor.

132. Sasha Costanza Chock, "Design Justice: Towards an Intersectional Feminist Framework for Design Theory and Practice," *Proceedings of the Design Research Society 2018*, June 3, 2018, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3189696.

133. Fight for the Future, "An Open Letter to Salesforce: Drop Your Contract with CBP," Medium, July 17, 2018, https://medium.com/@fightfortheftr/an-open-letter-to-salesforce-drop-your-contract-with-cbp-a8260841b627.

134. Sheera Frenkel, "Microsoft Employees Question C.E.O. Over Company's Contract With ICE," *New York Times,* July 26, 2018, https://www.nytimes.com/2018/07/26/technology/microsoft-ice-immigration.html.

135. Bryan Menegus, "Accenture Employees Demand Their Company Break Ties With U.S. Border Patrol," *Gizmodo,* November 15, 2018, https://gizmodo.com/accenture-employees-demand-their-company-break-ties-wit-1830474961.

136. Colin Lecher, "Google Employees 'Refuse to Be Complicit' in Border Agency Cloud Contract," *The Verge, August 14, 2019, https://www.theverge.com/2019/8/14/20805432/google-employees-petition-protest-customs-border-cloud-computing-contract*.

137. Lauren Kaori Gurley, "Tech Workers Walked Off the Job after Software They Made Was Sold to ICE," *Motherboard,* October 31, 2019, https://www.vice.com/en_us/article/43k8mp/tech-workers-walked-off-the-job-after-software-they-made-was-sold-to-ice.

138. Chris Merriman, "GitHub Devs Warn Microsoft 'Ditch That Contract with ICE or Lose Us,'" *Inquirer,* June 22, 2018, https://www.theinquirer.net/inquirer/news/3034641/github-devs-warn-microsoft-get-that-contract-on-ice-or-lose-us.

139. Ron Miller, "Programmer Who Took Down Open-Source Pieces over Chef ICE Contract Responds," *TechCrunch*, September 23, 2019, https://techcrunch.com/2019/09/23/programmer-who-took-down-open-source-pieces-over-chef-ice-contract-responds/.

140. See Douglas MacMillan and Elizabeth Dwoskin, "The War inside Palantir: Data-Mining Firm's Ties to ICE under Attack by Employees," *Washington Post,* August 22, 2019, https://www.washingtonpost.com/business/2019/08/22/war-inside-palantir-data-mining-firms-ties-ice-under-attack-by-employees/; and Rosalie Chan, "Palantir Workers Are Split over the Company's Work with ICE, but CEO Alex Karp Won't Budge despite Concerned Employees' Petitions," *Business Insider,* August 22, 2019, https://www.businessinsider.com/palantir-employees-ice-petition-alex-karp-2019-8.

141. Alex Karp, "I'm a Tech CEO, and I Don't Think Tech CEOs Should Be Making Policy," *Washington Post,* September 5, 2019, https://www.washingtonpost.com/opinions/policy-decisions-should-be-made-by-elected-representatives-not-silicon-valley/2019/09/05/e02a38dc-cf61-11e9-87fa-8501a456c003_story.html.

142. Alie Breland, "ICE Accidentally Just Revealed How Much Its New Contract With Peter Thiel's Palantir Is Worth," *Mother Jones,* August 20, 2019, https://www.motherjones.com/politics/2019/08/ice-palantir-contract-amount-revealed/.

143. Microsoft Employees, "An Open Letter to Microsoft: Don't Bid on the US Military's Project JEDI," Medium, October 12, 2018, https://medium.com/s/story/an-open-letter-to-microsoft-dont-bid-on-the-us-military-s-project-jedi-7279338b7132.

144. Microsoft Workers 4 Good (@MSWorkers4), "On behalf of workers at Microsoft, we're releasing an open letter to Brad Smith and Satya Nadella, demanding for [sic] the cancelation of the IVAS contract with a call for stricter ethical guidelines," Twitter, February 22, 2019, https://twitter.com/MsWorkers4/status/1099066343523930112.

145. Silicon Valley Rising, "Google Shareholder Meeting," June 19, 2019, https://act.siliconvalleyrising.org/google_shareholder_meeting.

146. Google Walkout for Real Change, "Not OK, Google," Medium, April 2, 2019, https://medium.com/@GoogleWalkout/not-ok-google-79cc63342c05.

147. Amazon Employees for Climate Justice, "Open letter to Jeff Bezos and the Amazon Board of Directors," Medium, April 10, 2019, https://medium.com/@amazonemployeesclimatejustice/public-letter-to-jeff-bezos-and-the-amazon-board-of-directors-82a8405f5e38.

148. Louise Matsakis, "Amazon Employees Will Walk Out over the Company's Climate Change Inaction," *Wired,* September 9, 2019, https://www.wired.com/story/amazon-walkout-climate-change/.

149. Dave Lee, "Google Staff Walk Out over Women's Treatment," BBC, November 1, 2018, https://www.bbc.com/news/technology-46054202.

150. Nathan Grayson and Cecilia D'Anastasio, "Over 150 Riot Employees Walk Out to Protest Forced Arbitration and Sexist Culture," *Kotaku,* May 6, 2019, https://kotaku.com/over-150-riot-employees-walk-out-to-protest-forced-arbi-1834566198.

151. Tracy Qu, "How GitHub Became a Bulletin Board for Chinese Tech Worker Complaints," *Quartz,* April 9, 2019, https://qz.com/1589309/996-icu-github-hosts-chinese-tech-worker-complaints/.

152. Johana Bhuiyan, "Google Workers Protest Suspensions of Activist Employees," *Los Angeles Times*, November 22, 2019, https://www.latimes.com/business/technology/story/2019-11-22/google-workers-rally-activists-protests.

153. Kate Conger and Daisuke Wakabayashi, "Google Fires 4 Workers Active in Labor Organizing," *New York Times,* November 25, 2019, https://www.nytimes.com/2019/11/25/technology/google-fires-workers.html.

154. See Steven Greenhouse, "Facebook's Shuttle Bus Drivers Seek to Unionize," *New York Times,* October 5, 2014, https://www.nytimes.com/2014/10/06/business/facebooks-bus-drivers-seek-union.html; Mark Harris, "Amazon's Mechanical Turk Workers Protest: 'I Am a Human Being, Not an Algorithm,'" *Guardian,* December 3, 2014, https://www.theguardian.com/technology/2014/dec/03/amazon-mechanical-turk-workers-protest-jeff-bezos; Josh Eidelson, "Microsoft's Unionized Contract Workers Get Aggressive," April 30, 2015, https://www.bloomberg.com/news/articles/2015-04-30/microsoft-contract-workers-are-organizing; and Kia Kokalitcheva, "These Google Workers Have Voted to Join the Teamsters Union," *Fortune*, August 21, 2015, https://fortune.com/2015/08/21/these-google-workers-have-voted-to-join-the-teamsters-union/.

155. Working Partnerships USA, "Tech's Invisible Workforce," March, 2016, accessed November 22, 2019, https://www.wpusa.org/files/reports/TechsInvisibleWorkforce.pdf.

156. Alexia Fernández Campbell, "Google's Contractors Accuse CEO of Creating Unequal Workforce," *Vox*, December 7, 2018, https://www.vox.com/2018/12/7/18128922/google-contract-workers-ceo-sundar-pichai.

157. Phoebe Zhang, "Chinese Workers at Apple Supplier Foxconn Stage Street Protest over Unpaid Bonuses," *South China Morning Post,* December 16, 2018, https://www.scmp.com/news/china/article/2178201/chinese-workers-apple-supplier-foxconn-stage-street-protest-over-unpaid.

158. Josh Dzieza, "'Beat the Machine': Amazon Warehouse Workers Strike to Protest Inhumane Conditions," *The Verge*, July 16, 2019, https://www.theverge.com/2019/7/16/20696154/amazon-prime-day-2019-strike-warehouse-workers-inhumane-conditions-the-rate-productivity.

159. Nick Statt, "Whole Foods Employees Demand Amazon Break All Ties with ICE and Palantir," *The Verge,* August 12, 2019, https://www.theverge.com/2019/8/12/20802893/whole-foods-employees-amazon-ice-protest-palantir-facial-recognition.

160. Bryan Menegus, "Amazon's Aggressive Anti-Union Tactics Revealed in Leaked 45-Minute Video," *Gizmodo,* September 26, 2018, https://gizmodo.com/amazons-aggressive-anti-union-tactics-revealed-in-leake-1829305201.

161. Kate Conger, "Food Service Workers at Airbnb Have Unionized," *Gizmodo,* February 15, 2018, https://gizmodo.com/food-service-workers-at-airbnb-have-unionized-1823049379.

162. Alex Heath, "Facebook Cafeteria Workers Vote to Unionize, Demand Higher Wages," *Business Insider*, July 24, 2017, https://www.businessinsider.com/facebook-cafeteria-workers-unionize-demand-higher-wages-2017-7.

163. Unite Here, "Cafeteria Workers at Yahoo Unionize, Join Workers' Movement for Equality in the Tech Industry," Unite Here, December 13, 2017, http://unitehere.org/cafeteria-workers-at-yahoo-unionize/.

164. Josh Eidelson, "Union Power Is Putting Pressure on Silicon Valley's Tech Giants," *Bloomberg Businessweek,* September 14, 2017, https://www.bloomberg.com/news/articles/2017-09-14/union-power-is-putting-pressure-on-silicon-valley-s-tech-giants.

165. Reuters, "Amazon Holds Talks with Workers in Poland as Strike Threatened," Reuters, May 10, 2019, https://www.reuters.com/article/us-amazon-poland-wages/amazon-holds-talks-with-workers-in-poland-as-strike-threatened-idUSKCN1SG1I5.

166. Tekla Perry, "Startup Lanetix Pays US $775,000 to Software Engineers Fired for Union Organizing," *IEEE Spectrum,* November 12, 2018, https://spectrum.ieee.org/view-from-the-valley/at-work/tech-careers/startup-lanetix-pays-775000-to-software-engineers-fired-for-union-organizing.

167. Noam Scheiber and Daisuke Wakabayashi, "Google Hires Firm Known for Anti-Union Efforts," November 20, 2019, https://www.nytimes.com/2019/11/20/technology/Google-union-consultant.html.

168. Yaseen Aslam (@Yaseenaslam381), "Uber office in Paris has been occupied by drivers!" Twitter, November 20, 2019, 3:16 a.m., https://twitter.com/Yaseenaslam381/status/1197111465007894529.

169. Pretty Diva (@wisequeeneth), "Protest against @Uber ongoing at Jabi lake mall Abuja @UberNigeria," Twitter, November 20, 2019, 2:42 a.m., https://twitter.com/wisequeeneth/status/1197102822292164609.

170. April S. Glaser, "The Ride-Hail Strike Got Just Enough Attention to Terrify Uber," *Slate,* May 9, 2019, https://slate.com/technology/2019/05/uber-strike-impact-gig-worker-protest.html.

171. Edward Ongweso Jr., "We Spoke to Uber Drivers Who Have Taken Over the Company's Offices in France," *Vice*, November 26, 2019, https://www.vice.com/amp/en_us/article/zmjadx/we-spoke-to-uber-drivers-who-have-taken-over-the-companys-offices-in-france.

172. People's Dispatch, "Uber, Ola Drivers to Go on Strike in India Seeking Safety Measures and City Taxi Permit," *People's Dispatch,* July 4, 2019, https://peoplesdispatch.org/2019/07/04/uber-ola-drivers-to-go-on-strike-in-india-seeking-safety-measures-and-city-taxi-permit/.

173. China Labour Bulletin, "The Shifting Patterns of Transport Worker Protests in China Present a Major Challenge to the Trade Union," *China Labour Bulletin,* November 18, 2019, https://clb.org.hk/content/shifting-patterns-transport-worker-protests-china-present-major-challenge-trade-union.

174. Kari Paul, "California Uber and Lyft Drivers Rally for Bill Granting Rights to Contract Workers," *Guardian*, August 27, 2019, https://www.theguardian.com/us-news/2019/aug/27/california-uber-and-lyft-drivers-rally-for-bill-granting-rights-to-contract-workers.

175. Andrew J. Hawkins, "Uber Argues Its Drivers Aren't Core to Its Business, Won't Reclassify Them as Employees," *The Verge*, September 11, 2019, https://www.theverge.com/2019/9/11/20861362/uber-ab5-tony-west-drivers-core-ride-share-business-california.

176. Carolyn Said, "AB5 Gig Work Bill: All Your Questions Answered," *San Francisco Chronicle,* September 16, 2019, https://www.sfchronicle.com/business/article/AB5-gig-work-bill-All-your-questions-answered-14441764.php.

177. Carolyn Said, "Uber: We'll Fight in Court to Keep Drivers as Independent Contractors," *San Francisco Chronicle,* September 11, 2019, https://www.sfchronicle.com/business/article/Uber-We-ll-fight-in-court-to-keep-drivers-as-14432241.php.

178. Matthew Haag and Patrick McGeehan, "Uber Fined $649 Million for Saying Drivers Aren't Employees," *New York Times,* November 14, 2019, https://www.nytimes.com/2019/11/14/nyregion/uber-new-jersey-drivers.html.

179. Daisuke Wakabayashi, "Google's Shadow Work Force: Temps Who Outnumber Full-Time Employees," *New York Times,* May 28, 2019, https://www.nytimes.com/2019/05/28/technology/google-temp-workers.html.

180. United States Senate, Letter to Sundar Pichai, July 25, 2019, https://int.nyt.com/data/documenthelper/1547-senate-democrats-letter-google-temporary-workers/1ad40d0ad9ac2286b911/optimized/full.pdf#page=1.

181. Varoon Mathur and Meredith Whittaker (AI Now Institute), "How To Interview a Tech Company: A Guide for Students," Medium, September 17, 2019, https://medium.com/@AINowInstitute/how-to-interview-a-tech-company-d4cc74b436e9.

182. Salvador Rodriguez, "Facebook Has Struggled to Hire Talent since the Cambridge Analytica Scandal, according to Recruiters Who Worked There," CNBC, May 16, 2019, https://www.cnbc.com/2019/05/16/facebook-has-struggled-to-recruit-since-cambridge-analytica-scandal.html.

183. MoveOn.org, "Sign the Petition: Students Pledge to Refrain from Interviewing with Google until Commitment Not to Pursue Future Tech Military Contracts (e.g. Project Maven)," accessed November 19, 2019, https://petitions.moveon.org/sign/students-pledge-to-refrain.

184. See April Glaser, "The Techlash Has Come to Stanford," *Slate*, August 8, 2019, https://slate.com/technology/2019/08/stanford-tech-students-backlash-google-facebook-palantir.html; Shirin Ghaffary, "At UC Berkeley, Brown, and Yale, Students Are Fighting to Keep Palantir off Campus over Its ICE Contracts," *Recode*, September 26, 2019, https://www.vox.com/recode/2019/9/26/20884182/palantir-ice-protests-campus-family-separation-berkeley-yale-brown; Sebastian Cahill and Olivia Buccieri, "UC Berkeley Students Protest Amazon's Ties with ICE," *Daily Californian*, September 27, 2019, https://www.dailycal.org/2019/09/27/uc-berkeley-students-protest-amazons-ties-with-ice/; and Caroline O'Donovan, "Student Groups Don't Want Salesforce and Palantir on Campus," *Buzzfeed*, February 28, 2019, https://www.buzzfeednews.com/article/carolineodonovan/student-groups-protest-salesforce-palantir-ice-campus.

185. Mijente, "1,200+ Students at 17 Universities Launch Campaign Targeting Palantir," #NoTechForICE, September 16, 2019, https://notechforice.com/20190916-2/.

186. Courtney Linder, "Some Students, Faculty Remain Uneasy about CMU's Army AI Task Force," *Pittsburgh Post-Gazette*, February 18, 2019, https://www.post-gazette.com/business/tech-news/2019/02/17/army-ai-task-force-pittsburgh-cmu-farnam-jahanian-military-google-project-maven/stories/201902150015.

187. See "Anti-CIA Student Protests," Brown University Library, https://library.brown.edu/create/protest6090/anti-cia-student-protests/; and "Students Protest CIA Recruiting," *Stanford Daily*, October 27, 1967, https://stanforddailyarchive.com/cgi-bin/stanford?a=d&d=stanford19671027-02.2.15&e=-------en-20-.

188. John Ruddy, "Voices of Protest at UConn: Exhibit Looks Back at Anti-vietnam War Upheaval on Campus," *The Day*, September 1, 2019, https://www.theday.com/article/20190901/ENT02/190909991.

189. Arwa Mboya, "Why Joi Ito Needs to Resign," *The Tech,* August 29, 2019, https://thetech.com/2019/08/29/joi-ito-needs-to-resign.

190. Ronan Farrow, "How an Élite University Research Center Concealed Its Relationship with Jeffrey Epstein," *The New Yorker,* September 6, 2019, https://www.newyorker.com/news/news-desk/how-an-elite-university-research-center-concealed-its-relationship-with-jeffrey-epstein.

191. Nicolas Stolte, "After Epstein Protest, MIT Students Host Community Forum," *Huntington News*, September 26, 2019, https://huntnewsnu.com/59840/city-pulse/after-epstein-protest-mit-students-host-community-forum/.

192. Kristina Chen, "Student Forum about MIT-Epstein Relations Held with Reif, Senior Admin Present," *The Tech*, October 3, 2019, https://thetech.com/2019/10/03/mit-epstein-student-forum.

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

194. This provision in the GDPR was used by journalists to study profiling by dating and social media apps. See Judith Duportail, "I Asked Tinder for My Data. It Sent Me 800 Pages of My Deepest, Darkest Secrets," *Guardian*, September 26 2017, https://www.theguardian.com/technology/2017/sep/26/tinder-personal-data-dating-app-messages-hacked-sold.

195. Andrew Selbst and Julia Powles, "Meaningful Information and the Right to Explanation," *International Data Privacy Law* 7, no. 4 (November 27, 2017): 233–242, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3039125.

196. See Lilian Edwards and Michael Veale, "Slave to the Algorithm? Why a 'Right to an Explanation' Is Probably Not the Remedy You Are Looking For" *Duke Law & Technology Review* 16, no.18, May 24, 2017, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2972855; and Margot Kaminski, "The GDPR's Version of Algorithmic Accountability," *JOTWELL*, August 16, 2018, https://cyber.jotwell.com/the-gdprs-version-of-algorithmic-accountability/.

197. Margot E. Kaminski and Gianclaudio Malgieri, "Algorithmic Impact Assessments under the GDPR: Producing Multi-layered Explanations," U of Colorado Law Legal Studies Research Paper No. 19-28, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3456224.

198. Graham Greenleaf, "Global Data Privacy Laws 2019: 132 National Laws & Many Bills," *Privacy Laws & Business International Report* 157 (May 29, 2019): 14–18, 2019, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3381593.

199. See Yomi Kazeem, "Kenya Is Stepping Up Its Citizens' Digital Security with a New EU-Inspired Data Protection Law," *Quartz Africa*, November 12, 2019; and Alice Munyua, "Kenya Considers Protection of Privacy and Personal Data," Mozilla Blog, January 2, 2019, https://blog.mozilla.org/netpolicy/2019/01/02/kenya-considers-protection-of-privacy-and-personal-data/.

200. Anna Carolina Cagnoni, "Brazilian Data Protection Law: A Complex Patchwork," IAPP Privacy Tracker, April 10, 2019, https://iapp.org/news/a/brazilian-data-protection-law-a-complex-patchwork/.

201. See "S.2577 - Data Broker Accountability and Transparency Act of 2019," https://www.congress.gov/bill/116th-congress/senate-bill/2577/text?q=%7B%22search%22%3A%5B%22data%22%5D%7D&r=20&s=7; "Following Equifax Settlement, Senators Markey, Blumenthal and Smith Reintroduce Legislation to Hold Data Broker Industry Accountable," Ed Markey, September 26, 2019, https://www.markey.senate.gov/news/press-releases/following-equifax-settlement-senators-markey-blumenthal-and-smith-reintroduce-legislation-to-hold-data-broker-industry-accountable; "S.1951 - Designing Accounting Safeguards To Help Broaden Oversight and Regulations on Data," https://www.congress.gov/bill/116th-congress/senate-bill/1951/related-bills?q=%7B%22search%22%3A%5B%22%5C%22Designing+Accounting+Safeguards+to+Help+Broaden+Oversight+And+Regulations+on+Dat

a%5C%22%22%5D%7D&r=1&s=9; "S.2658 - Augmenting Compatibility and Competition by Enabling Service Switching Act of 2019," https://www.congress.gov/bill/116th-congress/senate-bill/2658/text; "H.R.2013 - Information Transparency & Personal Data Control Act," https://www.congress.gov/bill/116th-congress/house-bill/2013?q=%7B%22search%22%3A%5B%22data%22%5D%7D&s=7&r=3; "H.R.4978 - Online Privacy Act of 2019," https://www.congress.gov/bill/116th-congress/house-bill/4978/text?q=%7B%22search%22%3A%5B%22algorithm%22%5D%7D&r=29&s=1; and "California Consumer Privacy Act (CCPA)," https://oag.ca.gov/privacy/ccpa.

202. Sandra Wachter, Brent Mittelstadt, and Luciano Floridi, "Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation," *International Data Privacy Law,* December 28, 2016, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2903469.

203. Andrew Selbst and Julia Powles, "Meaningful Information and the Right to Explanation," *International Data Privacy Law* 7, no. 4 (November 27, 2017): 233–242, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3039125.

204. See Mike Ananny and Kate Crawford, "Seeing without Knowing: Limitations of the Transparency Ideal and Its Application to Algorithmic Accountability," *New Media & Society*, December 13, 2016; Jenna Burrell, "How the Machine 'Thinks': Understanding Opacity in Machine Learning Algorithms," *Big Data & Society*, January 6, 2016; Christopher Kuner, Dan Jerker B. Svantesson, Fred H. Cate, Orla Lynskey, Christopher Millard, "Machine Learning with Personal Data: Is Data Protection Law Smart Enough to Meet the Challenge?," *International Data Privacy Law* 7, no. 1 (February 2017): 1–2, https://doi.org/10.1093/idpl/ipx003.

205. Sofia Edvardsen, "How to Interpret Sweden's First GDPR Fine on Facial Recognition in School," IAPP, August 27, 2019, https://iapp.org/news/a/how-to-interpret-swedens-first-gdpr-fine-on-facial-recognition-in-school/.

206. "CNIL Bans High Schools' Facial-Recognition Programs," IAPP, October 29, 2019, https://iapp.org/news/a/cnil-bans-high-school-facial-recognition-programs/.

207. Sarah Martin, "Committee Led by Coalition Rejects Facial Recognition Database in Surprise Move," *Guardian*, October 23, 2019, https://www.theguardian.com/australia-news/2019/oct/24/committee-led-by-coalition-rejects-facial-recognition-database-in-surprise-move.

208. Rachel Metz, "Beyond San Francisco, More Cities Are Saying No to Facial Recognition," *CNN Business*, July 17, 2019, https://www.cnn.com/2019/07/17/tech/cities-ban-facial-recognition/index.html.

209. S. 847 Commercial Facial Recognition Privacy Act of 2019, https://www.govinfo.gov/content/pkg/BILLS-116s847is/pdf/BILLS-116s847is.pdf.

210. Alfred Ng, "Facial Recognition Surveillance Would Require Warrant under Bipartisan Bill," CNET, November 14, 2019, https://www.cnet.com/news/facial-recognition-surveillance-would-require-warrant-under-bipartisan-bill/.

211. No Biometric Barriers Act, https://drive.google.com/file/d/1w4ee-poGkDJUkcEMTEAVqHNunplvR087/view.

212. See Caroline Spivack, "New Bill Would Ban Facial Recognition Technology from Public Housing," *Curbed*, July 29, 2019, https://ny.curbed.com/2019/7/29/8934279/bill-ban-facial-recognition-public-housing-brooklyn-nyc; and Elizabeth Kim, "Hell's Kitchen Landlord Sued for Keyless Entry System Agrees to Provide Keys," *Gothamist*,

May 8, 2019,
https://gothamist.com/news/hells-kitchen-landlord-sued-for-keyless-entry-system-agrees-to-provide-keys.

213. Sigal Samuel, "Facial Recognition Tech Is a Problem. Here's How the Democratic Candidates Plan to Tackle It," *Vox*, September 12, 2019,
https://www.vox.com/future-perfect/2019/8/21/20814153/facial-recognition-ban-bernie-sanders-elizabeth-warren-kamala-harris-julian-castro-cory-booker.

214. S. 5528, http://lawfilesext.leg.wa.gov/biennium/2019-20/Pdf/Bills/Senate%20Bills/5528.pdf.

215. Texas 503 Business and Commerce Code,
https://statutes.capitol.texas.gov/Docs/BC/htm/BC.503.htm.

216. See A.B. 1281, "Privacy: Facial Recognition Technology: Disclosure,"
https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201920200AB1281; and A.B. 1215, "Law Enforcement: Facial Recognition and Other Biometric Surveillance,"
https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201920200AB1215.

217. Arkansas Act 1030, https://legiscan.com/AR/bill/HB1943/2019.

218. NY S.B. 1203,
https://assembly.state.ny.us/leg/?default_fld=&leg_video=&bn=S01203&term=2019&Summary=Y&Text=Y; and A.B. A6787B, https://www.nysenate.gov/legislation/bills/2019/a6787.

219. Keep Internet Devices Safe Act,
http://www.ilga.gov/legislation/BillStatus.asp?DocNum=1719&GAID=15&DocTypeID=SB&SessionID=108&GA=101; Biometric Information Privacy Act (BIPA) from 2008,
http://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57.

220. Second Substitute Senate Bill 5376,
http://lawfilesext.leg.wa.gov/biennium/2019-20/Pdf/Bills/Senate%20Bills/5376-S2.pdf.

221. Michigan Senate Bill 342, https://legiscan.com/MI/bill/SB0342/2019.

222. AB-1215 Law Enforcement: Facial Recognition and Other Biometric Surveillance,
https://leginfo.legislature.ca.gov/faces/billCompareClient.xhtml?bill_id=201920200AB1215.

223. Bill S. 1385: An Act Establishing a Moratorium on Face Recognition and Other Remote Biometric Surveillance Systems, https://malegislature.gov/Bills/191/S1385/Bills/Joint.

224. Arizona House Bill 2478, https://legiscan.com/AZ/text/HB2478/id/1857901.

225. Florida House of Representatives, H.B. 1153,
https://www.flsenate.gov/Session/Bill/2019/1153/BillText/Filed/PDF.

226. *Patel v. Facebook, Inc.*, 932 F. 3d 1264 - Court of Appeals, 9th Circuit 2019,
https://scholar.google.com/scholar_case?case=9033020751616130750&hl=en&as_sdt=6&as_vis=1&oi=scholarr.

227. Brad Smith, "Facial Recognition: It's Time for Action," *Microsoft on the Issues*, December 6, 2018,
https://blogs.microsoft.com/on-the-issues/2018/12/06/facial-recognition-its-time-for-action/.

228. Michael Punke, "Some Thoughts on Facial Recognition Legislation," *AWS Machine Learning Blog*, February 7, 2019,
https://aws.amazon.com/blogs/machine-learning/some-thoughts-on-facial-recognition-legislation/.

229. Chris Burt, "Dueling Washington State Facial Recognition Bills Spark Regulation Debate," BiometricUpdate.com, February 21, 2019, https://www.biometricupdate.com/201902/duelling-washington-state-facial-recognition-bills-spark-regulation-debate.

230. Steve Dent, "Amazon Shareholders Will Vote to Ban Facial Recognition Tech," *Engadget*, April 15, 2019, https://www.engadget.com/2019/04/15/amazon-shareholder-vote-facial-recognition/.

231. Zack Whittaker, "Amazon Defeated Shareholder's Vote on Facial Recognition by a Wide Margin," *TechCrunch*, May 28, 2019, https://techcrunch.com/2019/05/28/amazon-facial-recognition-vote/.

232. Charlie Warzel, "A Major Police Body Cam Company Just Banned Facial Recognition," *New York Times*, June 27, 2019, https://www.nytimes.com/2019/06/27/opinion/police-cam-facial-recognition.html.

233. Helene Fouquet, "France Set to Roll Out Nationwide Facial Recognition ID Program," *Bloomberg*, October 3, 2019, https://www.bloomberg.com/news/articles/2019-10-03/french-liberte-tested-by-nationwide-facial-recognition-id-plan.

234. See, for example, Liberty, "Resist Facial Recognition," https://www.libertyhumanrights.org.uk/resist-facial-recognition; Big Brother Watch, "Face Off," May 2019, https://bigbrotherwatch.org.uk/all-campaigns/face-off-campaign/; Pete Fussey and Daragh Murray, "Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology," Human Rights, Big Data and Technology Project, 2019, https://www.hrbdt.ac.uk/download/independent-report-on-the-london-metropolitan-police-services-trial-of-live-facial-recognition-technology/; Owen Bowcott, "Police Face Legal Action over Use of Facial Recognition Cameras," *Guardian*, June 14, 2018, https://www.theguardian.com/technology/2018/jun/14/police-face-legal-action-over-use-of-facial-recognition-cameras; and Sarah Marsh, "Ethics Committee Raises Alarm over 'Predictive Policing' Tool," *Guardian*, April 20, 2019, https://www.theguardian.com/uk-news/2019/apr/20/predictive-policing-tool-could-entrench-bias-ethics-committee-warns.

235. Paul Mozur, "One Month, 500,000 Face Scans: How China Is Using A.I. to Profile a Minority," *New York Times*, April 14, 2019, https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html.

236. Paul Mozur, "In Hong Kong Protests, Faces Become Weapons," *New York Times*, July 26, 2019, https://www.nytimes.com/2019/07/26/technology/hong-kong-protests-facial-recognition-surveillance.html.

237. "The Personal Data (Privacy) Ordinance," PCPD, https://www.pcpd.org.hk/english/data_privacy_law/ordinance_at_a_Glance/ordinance.html.

238. Meredith Whittaker, Kate Crawford, Roel Dobbe, Genevieve Fried, Elizabeth Kazunias, Varoon Mathur, Sarah Myers West, Rashida Richardson, Jason Schultz, and Oscar Schwartz, "AI Now Report 2018," AI Now Institute, https://ainowinstitute.org/AI_Now_2018_Report.pdf, 22.

239. See also Andrew Selbst, "Accountable Algorithmic Futures: Building Empirical Research into the Future of the Algorithmic Accountability Act," *Data & Society: Points*, April 19, 2019, https://points.datasociety.net/building-empirical-research-into-the-future-of-algorithmic-accountability-act-d230183bb826; Alessandro Mantelero, "AI and Big Data: A Blueprint for a Human Rights, Social and Ethical Impact Assessment," *Computer Law & Security Review* 34 no. 4 (August 2018): 754–772,

https://www.sciencedirect.com/science/article/pii/S0267364918302012; and "AI Now Report 2018," https://ainowinstitute.org/AI_Now_2018_Report.pdf.

240. Reisman et al., "Algorithmic Impact Assessments: A Practical Framework for Public Agency Accountability," https://ainowinstitute.org/aiareport2018.pdf.

241. "Directive on Automated Decision-Making," Government of Canada, February 5, 2019, https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=32592.

242. D. Dawson, E. Schleiger, et al., "Artificial Intelligence: Australia's Ethics Framework," Commonwealth Scientific and Industrial Research Organisation, April 2019, https://consult.industry.gov.au/strategic-policy/artificial-intelligence-ethics-framework/supporting_documents/ArtificialIntelligenceethicsframeworkdiscussionpaper.pdf.

243. Washington House Bill 1655, https://legiscan.com/WA/bill/HB1655/2019.

244. Washington SB 5527 - 2019-20, https://app.leg.wa.gov/billsummary?BillNumber=5527&Year=2019.

245. TAP Staff, "How the GDPR Approaches Algorithmic Accountability," Technology | Academics | Policy, November 8, 2019, http://www.techpolicy.com/Blog/Featured-Blog-Post/How-the-GDPR-Approaches-Algorithmic-Accountability.aspx.

246. "Rep. Takano Introduces the Justice in Forensic Algorithms Act to Protect Defendants' Due Process Rights in the Criminal Justice System," Takano, September 17, 2019, https://takano.house.gov/newsroom/press-releases/rep-takano-introduces-the-justice-in-forensic-algorithms-act-to-protect-defendants-due-process-rights-in-the-criminal-justice-system.

247. S. 6428, which creates a statewide task force to examine the role of automated decision systems in government, is pending legislation. Whereas S. 3971B/A.1746C, which creates a temporary state commission to study and investigate how to regulate artificial intelligence, robotics, and automation, was signed into law and only includes government officials. The commission has not yet commenced.

248. "New York City Automated Decision Systems Task Force Report," November 2019, https://www1.nyc.gov/assets/adstaskforce/downloads/pdf/ADS-Report-11192019.pdf; "Executive Order 50 of November 19, 2019, Establishing An Algorithms Management and Policy Officer," November 19, 2019, https://www1.nyc.gov/assets/home/downloads/pdf/executive-orders/2019/eo-50.pdf.

249. A Local Law to amend the administrative code of the City of New York, in relation to reporting on automated decision systems used by city agencies, Int. 1806-2019, https://legistar.council.nyc.gov/LegislationDetail.aspx?ID=4265421&GUID=FBA29B34-9266-4B52-B438-A772D81B1CB5&Options=&Search=; Rashida Richardson, ed., "Confronting Black Boxes: A Shadow Report of the New York City Automated Decision System Task Force," AI Now Institute, December 4, 2019, https://ainowinstitute.org/ads-shadowreport-2019.pdf.

250. For more information, see Rashida Richardson, Jason M. Schultz, and Vincent M. Southerland, "Litigating Algorithms," AI Now Institute, September 2019, https://ainowinstitute.org/litigatingalgorithms-2019-us.pdf.

251. AI Now Institute, "Litigating Algorithms, September 2018, https://ainowinstitute.org/litigatingalgorithms.pdf.

252. Dave Dormer, "Red Deer RCMP Launch Voluntary Surveillance Camera Registry," CTV News, July 8, 2019,

https://calgary.ctvnews.ca/mobile/red-deer-rcmp-launch-voluntary-surveillance-camera-registry-1.4499224?cache=yes?clipId=89680.

253. Karen Bartko, "Over 160 Properties Join Red Deer Surveillance Camera Registry in First 4 Months," *Global News,* November 13, 2019, https://globalnews.ca/news/6163354/red-deer-surveillance-camera-registry/.

254. Allie Gross, "City Asks Detroiters to Support New Neighborhood Surveillance," *Detroit Free Press,* March 21, 2019, https://www.freep.com/story/news/local/michigan/detroit/2019/03/21/detroit-surveillance-program/3204549002/; Aaron Mondry, "Criticism Mounts over Detroit Police Department's Facial Recognition Software," *Curbed,* July 8, 2019, https://detroit.curbed.com/2019/7/8/20687045/project-green-light-detroit-facial-recognition-technology.

255. Neighbors by Ring, accessed November 20, 2019, https://www.amazon.com/Ring-Neighbors-by/dp/B07V7K49QT.

256. Caroline Haskins, "Amazon Is Coaching Cops on How to Obtain Surveillance Footage without a Warrant," *Motherboard,* August 5, 2019, https://www.vice.com/en_us/article/43kga3/amazon-is-coaching-cops-on-how-to-obtain-surveillance-footage-without-a-warrant.

257. Haskins, "Amazon Is Coaching Cops on How to Obtain Surveillance Footage without a Warrant."

258. Haskins, "Amazon Is Coaching Cops on How to Obtain Surveillance Footage without a Warrant."

259. Jessi Hempel, "For Nextdoor, Eliminating Racism Is No Quick Fix," *Wired,* February 16, 2017, https://www.wired.com/2017/02/for-nextdoor-eliminating-racism-is-no-quick-fix/.

260. Rani Molla, "The Rise of Fear-Based Social Media Like Nextdoor, Citizen, and Now Amazon's Neighbors," *Recode,* May 7, 2019, https://www.vox.com/recode/2019/5/7/18528014/fear-social-media-nextdoor-citizen-amazon-ring-neighbors.

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

262. Jathan Sadowski and Roy Bendor, "Selling Smartness: Corporate Narratives and the Smart City as a Sociotechnical Imaginary," *Science, Technology, & Human Values* 44, no. 3 (May 2019): 540–63, https://doi.org/10.1177%2F0162243918806061.

263. Molly Sauter, "City Planning Heaven Sent," *e-flux*, February 1, 2019, https://www.e-flux.com/architecture/becoming-digital/248075/city-planning-heaven-sent/.

264. Grand View Research, "Smart Cities Market Size Worth $237.6 Billion By 2025," May 2019, https://www.grandviewresearch.com/press-release/global-smart-cities-market.

265. Sidewalk Labs, "Vision Sections of RFP Submission," October 17, 2017, http://www.passivehousecanada.com/wp-content/uploads/2017/12/TO-Sidewalk-Labs-Vision-Sections-of-RFP-Submission-sm.pdf.

266. Lauren Feiner, "Alphabet's Sidewalk Labs Wants a Cut of Toronto Taxes to Build a Smart City There," CNBC, February 15, 2019, https://www.cnbc.com/2019/02/15/alphabets-sidewalk-labs-wants-a-cut-of-toronto-taxes-for-smart-city.html.

267. Sidewalk Labs, "MIDP," June 24, 2019, https://www.sidewalktoronto.ca/midp/.

268. Robert Brauneis and Ellen P. Goodman, "Algorithmic Transparency for the Smart City," *Yale Journal of Law & Technology* 20, no.103 (2018), https://yjolt.org/algorithmic-transparency-smart-city.

269. Bianca Wylie, "Debrief on Sidewalk Toronto Public Meeting #3 - A Master Class in Gaslighting and Arrogance," Medium, August 19, 2018, https://medium.com/@biancawylie/debrief-on-sidewalk-toronto-public-meeting-3-a-master-class-in-gaslighting-and-arrogance-c1c5dd918c16.

270. Kate Kaye, "What's Hidden in a Sidewalk Labs Government Contract," *RedTail*, July 26, 2019, https://redtailmedia.org/2019/07/26/heres-what-a-sidewalk-labs-contract-looks-like/.

271. Cathrin Schaer, "A German City of Industry Gets a Modern Makeover," *CityLab*, September 19, 2019, https://www.citylab.com/life/2019/09/berlin-smart-city-siemens-siemensstadt-project-data-privacy/597514/.

272. Clare Garvie and Laura M. Moy, "America Under Watch: Face Surveillance in the United States," *The Center on Privacy & Technology at Georgetown Law*, May 16, 2019, https://www.americaunderwatch.com.

273. Jean Marie Takouleu, "AFRICA: Huawei sets up a $1.5 billion fund to boost African smart cities," Afrik 21, October 2, 2019, https://www.afrik21.africa/en/africa-huawei-sets-up-a-1-5-billion-fund-to-boost-african-smart-cities/.

274. "Video Surveillance as the Foundation of 'Safe City' in Kenya," Huawei, https://www.huawei.com/en/industry-insights/technology/digital-transformation/video/video-surveillance-as-the-foundation-of-safe-city-in-kenya.

275. Joe Parkinson, Nicholas Bariyo, and Josh Chin, "Huawei Technicians Helped African Governments Spy on Political Opponents," *Wall Street Journal*, August 15, 2019, https://www.wsj.com/articles/huawei-technicians-helped-african-governments-spy-on-political-opponents-11565793017.

276. Joshua Emerson Smith, "As San Diego Increases Use of Streetlamp Cameras, ACLU Raises Surveillance Concerns," *Los Angeles Times*, August 5, 2019, https://www.latimes.com/california/story/2019-08-05/san-diego-police-ramp-up-use-of-streetlamp-cameras-to-crack-cases-privacy-groups-raise-concerns.

277. Daniel Rivero, "Miami Could Let Company Put Surveillance Poles on Public Property for Free," WLRN, October 9, 2019, https://www.wlrn.org/post/miami-could-let-company-put-surveillance-poles-public-property-free.

278. Caroline Haskins, "300 Californian Cities Secretly Have Access to Palantir," *Motherboard*, July 12, 2019, https://www.vice.com/en_us/article/neapqg/300-californian-cities-secretly-have-access-to-palantir.

279. BlockSidewalk, "BlockSidewalk," February 25, 2019, https://www.blocksidewalk.ca.

280. Block Sidewalk, "Media releases," June 24, 2019, https://www.blocksidewalk.ca/media.

281. Canadian Civil Liberties Association, "CCLA Commences Proceedings Against Waterfront Toronto," April 16, 2019, https://ccla.org/ccla-commences-proceedings-waterfront-toronto/.

282. He also noted that the proposal requires unreasonable government commitments (such as creating new roles for public administrators and changing regulations). Steve Diamond, "Open Letter from Waterfront Toronto Board Chair, Stephen Diamond Regarding Quayside," June 24, 2019,

https://quaysideto.ca/wp-content/uploads/2019/06/Open-Letter-from-WT-Board-Chair-on-Quayside-June-24-FINAL.pdf.

283. Waterfront Toronto, "Overview of Realignment of MIDP Threshold Issues," https://quaysideto.ca/wp-content/uploads/2019/10/Overview-of-Thresold-Issue-Resolution-Oct-29.pdf.

284. George Zegarac, "Re: Plan Development Agreement Threshold Issues," October 29, 2019, https://waterfrontoronto.ca/nbe/wcm/connect/waterfront/86d92f81-20be-4029-a616-00522abbd34a/Concurrence+Letter.pdf?MOD=AJPERES.

285. See Shirin Ghaffery, "The 'Smarter' Wall: How Drones, Sensors, and AI Are Patrolling the Border," *Recode*, May 16, 2019, https://www.vox.com/recode/2019/5/16/18511583/smart-border-wall-drones-sensors-ai; and Leigh Ann Caldwell, Kasie Hunt, and Rebecca Shabad, "Top House Dem Says New Offer Will Focus on Funding 'Smart Wall'," NBC News, January 23, 2019, https://www.nbcnews.com/politics/congress/top-house-dem-says-new-offer-will-focus-funding-smart-n961746.

286. Lee Fang, "Defense Tech Startup Founded by Trump's Most Prominent Silicon Valley Supporters Wins Secretive Military AI Contract," *The Intercept*, March 9, 2019, https://theintercept.com/2019/03/09/anduril-industries-project-maven-palmer-luckey/.

287. Sam Dean, "A 26-Year-Old Billionaire Is Building Virtual Border Walls—and the Federal Government Is Buying," *Los Angeles Times*, July 26, 2019, https://www.latimes.com/business/story/2019-07-25/anduril-profile-palmer-luckey-border-controversy.

288. Mijente, "The War against Immigrants: Trump's Tech Tools Powered by Palantir," August 2019, https://mijente.net/wp-content/uploads/2019/08/Mijente-The-War-Against-Immigrants_-Trumps-Tech-Tools-Powered-by-Palantir_.pdf.

289. Drew Harwell, "FBI, ICE Find State Driver's License Photos Are a Gold Mine for Facial-Recognition Searches," *Washington Post*, July 7, 2019, https://www.washingtonpost.com/technology/2019/07/07/fbi-ice-find-state-drivers-license-photos-are-gold-mine-facial-recognition-searches/.

290. Bobby Allyn and Joel Rose, "Justice Department Announces Plan to Collect DNA from Migrants Crossing the Border," NPR, October 21, 2019, https://www.npr.org/2019/10/21/772035602/justice-department-announces-plan-to-collect-dna-from-migrants-crossing-the-bord.

291. Dani Deahl, "The EU Plans to Test an AI Lie Detector at Border Points," *The Verge*, October 31, 2018, https://www.theverge.com/2018/10/31/18049906/eu-artificial-intelligence-ai-lie-detector-border-points-immigration.

292. Diane Taylor, "Border Control Systems Face Fire from Travellers Wrongly Delayed," *Guardian*, September 7, 2019, https://www.theguardian.com/politics/2019/sep/07/border-control-systems-face-fire-from-travellers-wrongly-delayed.

293. Olivia Solon, "Why Did Microsoft Fund an Israeli Firm That Surveils West Bank Palestinians?," NBC News, October 28, 2019, https://www.nbcnews.com/news/all/why-did-microsoft-fund-israeli-firm-surveils-west-bank-palestinians-n1072116.

294. Sue-Lin Wong and Qianer Liu, "Emotion Recognition Is China's New Surveillance Craze," *Financial Times*, October 31, 2019, https://www.ft.com/content/68155560-fbd1-11e9-a354-36acbbb0d9b6.

295. ACLU, "The Constitution in the 100-Mile Border Zone," August 21, 2014, https://www.aclu.org/other/constitution-100-mile-border-zone.

296. See Carly Nyst et al., "Digital Identity: Issue Analysis," Consult Hyperion for Omidyar Network, June 8, 2016, http://www.chyp.com/wp-content/uploads/2016/07/PRJ.1578-Digital-Identity-Issue-Analysis-Report-v1_6-1.pdf; and Zara Rahman, "Digital ID: Why It Matters, and What We're Doing about It," Engine Room, September 13, 2018, https://www.theengineroom.org/digital-id-why-it-matters/.

297. ID4D, "Identification for Development," World Bank, accessed November 21, 2019 https://id4d.worldbank.org/.

298. "The Sustainable Development Goals, Identity, and Privacy: Does Their Implementation Risk Human Rights?," Privacy International, August 29, 2018, https://privacyinternational.org/long-read/2237/sustainable-development-goals-identity-and-privacy-does-their-implementation-risk.

299. See Aria Thaker, "The New Oil: Aadhaar's Mixing of Public Risk and Private Profit," *Caravan*, April 30, 2018, https://caravanmagazine.in/reportage/aadhaar-mixing-public-risk-private-profit; Usha Ramanathan, "Who Owns the UID Database?," MediaNama, May 6, 2013, https://www.medianama.com/2013/05/223-who-owns-the-uid-database-usha-ramanathan/; and Pam Dixon, "A Failure to 'Do No Harm'—India's Aadhaar Biometric ID Program and Its Inability to Protect Privacy in Relation to Measures in Europe and the U.S.," *Health and Technology* 7, no. 6 (June 2017), https://doi.org/10.1007/s12553-017-0202-6.

300. Vindu Goel, "India's Top Court Limits Sweep of Biometric ID Program," *New York Times*, September 26, 2018, https://www.nytimes.com/2018/09/26/technology/india-id-aadhaar-supreme-court.html.

301. Nicolas Kayser-Bril, "Identity-Management and Citizen Scoring in Ghana, Rwanda, Tunisia, Uganda, Zimbabwe and China," Algorithm Watch, October 22, 2019, https://algorithmwatch.org/wp-content/uploads/2019/10/Identity-management-and-citizen-scoring-in-Ghana-Rwanda-Tunesia-Uganda-Zimbabwe-and-China-report-by-AlgorithmWatch-2019.pdf.

302. See Emrys Schoemaker, Tom Kirk, and Isaac Rutenberg, *Kenya's Identity Ecosystem* (Farnham, Surrey, United Kingdom: Caribou Digital Publishing, 2019), https://www.cariboudigital.net/wp-content/uploads/2019/10/Kenyas-Identity-Ecosystem.pdf; and Jyoti Panday, "Can India's Biometric Identity Program Aadhaar Be Fixed?," Electronic Frontier Foundation, February 27, 2018, https://www.eff.org/deeplinks/2018/02/can-indias-aadhaar-biometric-identity-program-be-fixed.

303. Rachna Khaira, Aman Sethi, and Gopal Sathe, "UIDAI's Aadhaar Software Hacked, ID Database Compromised, Experts Confirm," *Huffington Post India*, September 11, 2018, https://www.huffingtonpost.in/2018/09/11/uidai-s-aadhaar-software-hacked-id-database-compromised-experts-confirm_a_23522472/.

304. Richard Milne and Michael Peel, "Red Faces in Estonia over ID Card Security Flaw," *Financial Times*, September 5, 2017, https://www.ft.com/content/874359dc-925b-11e7-a9e6-11d2f0ebb7f0.

305. Rasna Warah, "Huduma Namba: Another Tool to Oppress Kenyans?," *The Elephant*, April 20, 2019, https://www.theelephant.info/op-eds/2019/04/20/huduma-namba-another-tool-to-oppress-kenyans/.

306. See Rahul Lahoti, "Questioning the 'Phenomenal Success' of Aadhaar-linked Direct Benefit Transfers for LPG," *Economic & Political Weekly* 51, no. 52 (December 24, 2016),

https://www.epw.in/journal/2016/52/web-exclusives/questioning-%E2%80%9Cphenomenal-success%E2%80%9D-aadhaar-linked-direct-benefit; Reetika Khera, "The UID Project and Welfare Schemes," *Economic & Political Weekly* 46, no. 9 (February 26, 2011): 38–43, www.jstor.org/stable/41151836.

307. See Philip Alston, "Report of the Special Rapporteur on Extreme Poverty and Human Rights," October 11, 2019, https://srpovertyorg.files.wordpress.com/2019/10/a_74_48037_advanceuneditedversion-1.pdf; and "AI Now Report 2018," December 2018, https://ainowinstitute.org/AI_Now_2018_Report.pdf.

308. William Reuben and Flávia Carbonari, "Identification as a National Priority: The Unique Case of Peru," CGD Working Paper 454, Center for Global Development, May 11, 2017, https://www.cgdev.org/publication/identification-national-priority-unique-case-peru.

309. Jean Drèze, "Chronicle of a Starvation Death Foretold: Why It Is Time to Abandon Aadhaar in the Ration Shop," Scroll, October 21, 2017, https://scroll.in/article/854847/chronicle-of-a-starvation-death-foretold-why-it-is-time-to-abandon-aadhaar-in-the-ration-shop.

310. *Julian Robinson v. Attorney General of Jamaica* [2019] JMFC Full 04, https://supremecourt.gov.jm/sites/default/files/judgments/Robinson%2C%20Julian%20v%20Attorney%20General%20of%20Jamaica.pdf.

311. Jack Horgan-Jones, "Irish State Told to Delete 'Unlawful' Data on 3.2m Citizens," *Irish Times*, August 16, 2019, https://www.irishtimes.com/news/ireland/irish-news/irish-state-told-to-delete-unlawful-data-on-3-2m-citizens-1.3987606.

312. *K. S. Puttaswamy v. Union of India*, Supreme Court of India, Writ Petition (Civil) No. 494 of 2012, https://indiankanoon.org/doc/127517806/.

313. Nanjala Nyabola, "If You Are a Kenyan Citizen, Your Private Data Is Not Safe," *Al Jazeera*, February 24, 2019, https://www.aljazeera.com/indepth/opinion/kenyan-citizen-private-data-safe-190221150702238.html.

314. Chris Burt, "Brazil Plans Massive Centralized Biometric Database of All Citizens to Improve Agency Data Sharing," *Biometric Update*, October 15, 2019, https://www.biometricupdate.com/201910/brazil-plans-massive-centralized-biometric-database-of-all-citizens-to-improve-agency-data-sharing.

315. Helene Fouquet, "France Set to Roll Out Nationwide Facial Recognition ID Program," *Bloomberg*, October 3, 2019, https://www.bloomberg.com/news/articles/2019-10-03/french-liberte-tested-by-nationwide-facial-recognition-id-plan.

316. #WhyID, "An Open Letter to the Leaders of International Development Banks, the United Nations, International Aid Organisations, Funding Agencies, and National Governments," Access Now, https://www.accessnow.org/whyid-letter/.

317. "What to look for in digital identity systems: A typology of stages," The Engine Room, November 2019, https://www.theengineroom.org/wp-content/uploads/2019/10/Digital-ID-Typology-The-Engine-Room-2019.pdf.

318. Peter Asaro, "What Is an 'Artificial Intelligence Arms Race' Anyway?," *I/S: A Journal of Law and Policy* 15, nos. 1–2 (2019), https://moritzlaw.osu.edu/ostlj/wp-content/uploads/sites/125/2019/06/Asaro.pdf.

319. See "US, China Lead Race for Artificial Intelligence Patents: UN," Al Jazeera, January 31, 2019, https://www.aljazeera.com/news/2019/01/china-lead-race-artificial-intelligence-patents-19013108073254

8.html; Daniel Castro, Michael McLaughlin, and Eline Chivot, "Who Is Winning the AI Race: China, the EU or the United States?," Centre for Data Innovation, August 31, 2019, https://www.datainnovation.org/2019/08/who-is-winning-the-ai-race-china-the-eu-or-the-united-states/; and Tom Simonite, "China Is Catching Up to the US in AI Research—Fast," *Wired*, March 13, 2019, https://www.wired.com/story/china-catching-up-us-in-ai-research/.

320. Sarah O'Meara, "Will China Overtake the US in AI research?," *Scientific American*, August 24, 2019 https://www.scientificamerican.com/article/will-china-overtake-the-u-s-in-artificial-intelligence-research/.

321. Kai Fu Lee, "Why China Can Do AI More Quickly and Effectively than the US," *Wired*, October 23, 2018 https://www.wired.com/story/why-china-can-do-ai-more-quickly-and-effectively-than-the-us/.

322. See David Ignatius, "China's application of AI should be a Sputnik moment for the U.S. But will it be?," *Washington Post*, November 6, 2018, https://www.washingtonpost.com/opinions/chinas-application-of-ai-should-be-a-sputnik-moment-for-the-us-but-will-it-be/2018/11/06/69132de4-e204-11e8-b759-3d88a5ce9e19_story.html; "A Conversation With Ash Carter," Council on Foreign Relations, July 9, 2019, https://www.cfr.org/event/conversation-ash-carter; and Perry Chiaramonte, "Could China Leave the US Behind in AI 'Arms Race'?," Fox News, January 29, 2019, https://www.foxnews.com/tech/could-china-leave-the-us-behind-in-ai-arms-race.

323. See "Lt. Gen. Jack Shanahan Media Briefing on A.I.-Related Initiatives within the Department of Defense," US Department of Defense, August 30, 2019, https://www.defense.gov/Newsroom/Transcripts/Transcript/Article/1949362/lt-gen-jack-shanahan-media-briefing-on-ai-related-initiatives-within-the-depart/; and "Nuclear Posture Review," US Department of Defense, February 2018, https://media.defense.gov/2018/Feb/02/2001872886/-1/-1/1/2018-NUCLEAR-POSTURE-REVIEW-FINAL-REPORT.PDF. The Department also established the Defense Innovation Unit Experimental (DIUx) to foster closer collaboration between the Pentagon and Silicon Valley. Former Google CEO and current Chairman of the National Security Commision on Artificial Intelligence (NSCAI) Eric Schmidt, too, has been vocal about the importance of the US maintaining a strategic advantage in the "global competition for superior artificial intelligence."

324. See also Microsoft Employees, "An Open Letter to Microsoft: Don't Bid on the US Military's Project JEDI," Medium, October 12, 2018, https://medium.com/s/story/an-open-letter-to-microsoft-dont-bid-on-the-us-military-s-project-jedi-7279338b7132; and Lauren Gurley, "Tech Workers Walked Off the Job after Software They Made Was Sold to ICE," *Motherboard*, October 31, 2019 https://www.vice.com/en_us/article/43k8mp/tech-workers-walked-off-the-job-after-software-they-made-was-sold-to-ice.

325. Peter Thiel, "Good for Google, Bad for America," *New York Times*, August 1, 2019, https://www.nytimes.com/2019/08/01/opinion/peter-thiel-google.html; Alice Su, "The Question of 'Patriotism' in U.S.-China Tech Collaboration," *Los Angeles Times*, August 13, 2019, https://www.latimes.com/world-nation/story/2019-08-12/china-us-tech-patriotism-ethics-ai; Annie Palmer, "Palantir CEO Says Google Shouldn't Rule A.I.," CNBC, August 22, 2019, https://www.cnbc.com/2019/08/22/palantir-ceo-says-google-shouldnt-rule-ai.html.

326. Nicholas Thompson and Ian Bremmer, "The AI Cold War That Threatens US All", *Wired*, October 23, 2018, https://www.wired.com/story/ai-cold-war-china-could-doom-us-all/.

327. This is not dissimilar to the popular narrative that views privacy or due process safeguards as "friction" that impedes the ability for law enforcement or national security agencies to do their job effectively. See Lucia Zedner, "Too Much Security?," *International Journal of the Sociology of Law* 31, no. 3 (September 2003), 155–184, https://doi.org/10.1016/j.ijsl.2003.09.002.

328. "Up to one million detained in China's mass 're-education' drive," Amnesty International, August 2019, accessed November 26, 2019, https://www.amnesty.org/en/latest/news/2018/09/china-up-to-one-million-detained/.

329. Shazeda Ahmed, "Shazeda Ahmed on the Messy Truth about Social Credit," Berkeley School of Information, April 23 2019, https://www.ischool.berkeley.edu/news/2019/shazeda-ahmed-messy-truth-about-social-credit.

330. Abeba Birhane, "Situating China's Social Credit System in History and Context," August 8, 2018, https://abebabirhane.wordpress.com/2018/08/28/situating-chinas-social-credit-system-in-history-and-context/.

331. See Nick Couldry and Ulises Mejias, "Data Colonialism: Rethinking Big Data's Relation to the Contemporary Subject," *Television & New Media* 20, no. 4 (September 2018): 336–349, https://doi.org/10.1177/1527476418796632; Nick Couldry and Ulises Mejias, "Making Data Colonialism Liveable: How Might Data's Social Order Be Regulated?" *Internet Policy Review* 8, no. 2 (June 30, 2019), https://doi.org/10.14763/2019.2.1411; Jim Thatcher, David O'Sullivan, and Dillon Mahmoudi, "Data Colonialism through Accumulation by Dispossession: New Metaphors for Daily Data," *Society and Space* 34, no. 6 (2016): 990–1006, https://doi.org/10.1177%2F0263775816633195; and Ben Tarnoff, "The Data Is Ours!," *Logic*, April 1, 2018, https://logicmag.io/scale/the-data-is-ours/.

332. See, for example, DECODE, "Beyond Surveillance Capitalism: Reclaiming Digital Sovereignty," Decode Project Event, accessed November 20, 2019, https://decodeproject.eu/events/beyond-surveillance-capitalism-reclaiming-digital-sovereignty; CORDIS, "Digital Sovereignty: Power to the People", EC Cordis News, accessed November 20, 2019, https://cordis.europa.eu/article/rcn/123499/en.

333. "Mukesh Ambani says 'data colonisation' as bad as physical colonisation," *Economic Times*, December 19, 2018, https://economictimes.indiatimes.com/news/company/corporate-trends/mukesh-ambani-says-data-colonisation-as-bad-as-physical-colonisation/articleshow/67164810.cms; Government of India (DIPP), "Draft National e-Commerce Policy: India's Data for India's Development, February 2019, https://dipp.gov.in/sites/default/files/DraftNational_e-commerce_Policy_23February2019.pdf; United Nations Conference on Trade and Development, "Digital Economy Report 2019," https://unctad.org/en/pages/PublicationWebflyer.aspx?publicationid=2466.

334. For crucial work on technology, data, and postcolonial history, see Kavita Philip, *Civilizing Natures: Race, Resources, and Modernity in Colonial South India* (New Brunswick, NJ: Rutgers University Press, 2004); Benjamin Zachariah, "Uses of Scientific Argument: The Case of 'Development' in India, c 1930-1950," *Economic and Political Weekly* 36, no. 39 (2001): 3689–3702; Partha Chatterjee, *The Politics of the Governed: Reflections on Popular Politics in Most of the World* (New York: Columbia University Press: 2006); and Partha Chatterjee, *The Nation and Its Fragments: Colonial and Postcolonial Histories* (Princeton: Princeton University Press, 1993).

335. Sarah Roberts, *Behind the Screen: Content Moderation in the Shadows of Social Media* (New Haven, Yale University Press, 2019); Lilly Irani, "Difference and Dependence among Digital Workers: The Case of Amazon Mechanical Turk," *South Atlantic Quarterly* 114, no. 1 (January 2015): 225–234; Lilly Irani, *Chasing Innovation: Making Entrepreneurial Citizens in Modern India* (Princeton: Princeton University Press, 2019); Mary L. Gray and Siddharth Surl, *Ghost Work: How to Stop Silicon Valley from Building a New Global Underclass* (Boston: Houghton Mifflin Harcourt, 2019); Kate Crawford and Vladan Joler, Anatomy of an AI System, 2018, https://anatomyof.ai ; Muqing Zhang, "Colonialism Is Alive in the Exploited Tech Work Force", *Outline*, June 6, 2019 https://theoutline.com/post/7533/colonialism-is-alive-in-the-exploited-tech-work-force?zd=2&zi=exrbzkaf; APC, Article 19, and SIDA, "GISWatch 2019 - Artificial Intelligence: Human rights, social justice and development," November 2019, https://giswatch.org/sites/default/files/gisw2019_artificial_intelligence.pdf;

Noopur Raval, "Developing a Framework for Postcolonial Digital Labor," unpublished manuscript, 2017, https://www.academia.edu/35413303/Developing_a_framework_for_postcolonial_digital_labor.

336. Eve Tuck and Wayne Yang, "Decolonization Is Not a Metaphor," *Decolonization: Indigeneity, Education & Society* 1, no. 1 (2012), https://jps.library.utoronto.ca/index.php/des/article/view/18630**;** Monika Halkort, "On the Coloniality of Data Relations: Revisiting Data Colonialism as Research Paradigm," DATACTIVE, October 15, 2019, https://data-activism.net/2019/10/bigdatasur-on-the-coloniality-of-data-relations-revisiting-data-colonialism-as-research-paradigm-12; María Soledad Segura and Silvio Waisbord, "Between Data Capitalism and Data Citizenship," *Television & New Media* 20, no. 4 (2019),https://doi.org/10.1177/1527476419834519.

337. As scholar and activist Roxanne Dunbar-Ortiz has stated, there is an urgent need to address the core issue of settler colonialism as well as racism in Indigenous policy and advocacy. "US policies and actions related to Indigenous peoples," she writes, "though often termed 'racist' or 'discriminatory,' are rarely depicted as what they are: classic cases of imperialism and a particular form of colonialism—settler colonialism." See Dunbar-Ortiz, *An Indigenous Peoples' History of the United States* (Boston: Beacon Press, 2014), 2. See also Tahu Kukutai and John Taylor, eds., *Indigenous Data Sovereignty: Toward an Agenda* (Acton: The Australian National University Press, 2016); Stephanie Carroll Rainie, Jennifer Lee Schultz, Eileen Briggs, Patricia Riggs, and Nancy Lynn Palmanteer-Holder, "Data as a Strategic Resource: Self-Determination, Governance, and the Data Challenge for Indigenous Nations in the United States," *International Indigenous Policy Journal* 8, no. 2 (2017), http://dx.doi.org/10.18584/iipj.2017.8.2.1; Nick Estes, *Our History is The future: Standing Rock Versus the Dakota Access Pipeline, and the Long Tradition of Indigenous Resistance* (London: Verso Books, 2019).

338. For examples of this census administration, see National Congress of American Indians, "Census," accessed November 27, 2019, http://www.ncai.org/policy-issues/economic-development-commerce/census; and Statistics Canada, "Statistics on Indigenous Peoples," accessed November 27, 2019, https://www.statcan.gc.ca/eng/subjects-start/indigenous_peoples. This issue is especially pressing on the eve of the first digital US Census; see Issie Lapowsky, "The Challenge of America's First Online Census," *Wired*, February 6, 2019, https://www.wired.com/story/us-census-2020-goes-digital/https://www.wired.com/story/us-census-2020-goes-digital/. For critical historical reflections on US Census, see Dan Bouk, Census Stories, USA, https://censusstories.us/about/.

339. On settler-colonial water data and Navajo and Hopi resistance, see Theodora Dryer, "Computing Cloud Seeds: A Story of Anthropogenic Climate Change," in *Designing Certainty: The Rise of Algorithmic Computing in an Age of Anxiety* (PhD dissertation, University of California, San Diego, 2019). For crucial academic work on data and tech economies and questions of sovereignty and human rights, see Lisa Nakamura, "Indigenous Circuits: Navajo Women and the Racialization of Early Electronic Manufacture," *American Quarterly* 66, no. 4 (2014): 919–941; Kim TallBear, "Beyond the Life/Not Life Binary: A Feminist-Indigenous Reading of Cryopreservation, Interspecies Thinking and the New Materialisms," in *Cryopolitics: Frozen Life in a Melting World*, eds. Joanna Radin and Emma Kowal (Cambridge: MIT Press, 2017); Kim TallBear, "The Emergence, Politics, and Marketplace of Native American DNA," in *The Routledge Handbook of Science, Technology, and Society*, eds. Daniel Lee Kleinman and Kelly Moore (London: Routledge, 2014): 21–37; Eden Medina, *Cybernetic Revolutionaries: Technology and Politics in Allende's Chile* (Cambridge, MA: MIT Press, 2011); Eden Medina, "Forensic Identification in the Aftermath of Human Rights Crimes in Chile: A Decentered Computer History," *Technology & Culture* 59, no. 4 (2008): S100–S133; *Data Politics: Worlds, Subjects, Rights,* eds. Didier Bigo, Engin F. Isin, and Evelyn Ruppert (London: Routledge, 2019); Isaac Rivera, "Digital Enclosure and the Elimination of the Oceti Sakowin: The Case of the Dakota Access Pipeline," *Society + Space*, October 21, 2019, https://societyandspace.org/2019/10/21/digital-encosure-and-the-elimination-of-the-oceti-sakowin-the-cas

e-of-dapl/. For work on nonindegenous digital uses of Indigenous data, see Joanna Radin, "'Digital Natives': How Medical and Indigenous Histories Matter for Big Data," *Osiris* 32, no.1 (2017): 43–64.

340. For a comprehensive account on this, see Maggie Walter and Chris Anderson, *Indigenous Statistics: A Quantitative Research Methodology* (New York: Routledge, 2016). See also ABS, *Directions in Australia's Aboriginal and Torres Strait Islander Statistics* (Canberra: Australian Bureau of Statistics, 2007).

341. Native Nations Institute, "Indigenous Data Sovereignty and Governance," November 27, 2019, https://nni.arizona.edu/programs-projects/policy-analysis-research/indigenous-data-sovereignty-and-gover nance. For further reading, see Stephanie Carroll, Rainie, Desi Rodriguez-Lonebear, and Andrew Martinez, "Policy Brief: Indigenous Data Sovereignty in the United States," Native Nations Institute, University of Arizona, 2017; and Linda Tuhiwai Smith, *Decolonizing Methodologies: Research and Indigenous Peoples* (London: Zed Books, 2012).

342. See, for example, DECODE, "Data Sovereignty for the Sharing Economy: DECODE Project Kickoff, January 17, 2017, , https://capssi.eu/data-sovereignty-for-the-sharing-economy-decode-project-kickoff/; the UNCTAD Digital Economy Report (UNCTAD uses the term "indigenous innovation systems"), October 3, 2019, https://culture360.asef.org/resources/unctad-digital-economy-report-2019/; The European Observatory on Algorithmic Sovereignty, https://algosov.org/; and Renata Avila Pinto, "Digital Sovereignty or Digital Colonialism?," Sur International Journal on Human Rights, August 2019, https://sur.conectas.org/en/digital-sovereignty-or-digital-colonialism/.

343. Tahu Kukutai and John Taylor, eds., *Indigenous Data Sovereignty: Toward an Agenda* (Acton: The Australian National University Press, 2016).

344. Tahu Kukutai and John Taylor, *Indigenous Data Sovereignty*, xi.

345. For related literature, see Jane Anderson and Kimberly Christen, "Decolonizing Attribution: Traditions of Exclusion," *Journal of Radical Librarianship* 5 (2019); Rebecca Tsosie, "Tribal Data Governance and Informational Privacy: Constructing 'Indigenous Data Sovereignty'," *Montana Law Review* 229 (2019); Rosalina James et al., "Exploring Pathways to Trust: A Tribal Perspective on Data Sharing," *Genetics in Medicine* 16 (2014): 820–826.

346. Codirectors Jane Anderson and Kim Christen, Local Contexts, accessed November 27, 2019, https://localcontexts.org/.

347. Anderson and Christen, Local Contexts.

348. Library of Congress, Digital Collection, Ancestral Voices, accessed November 27, 2019, https://www.loc.gov/collections/ancestral-voices/about-this-collection/rights-and-access/.

349. Ancestral Voices.

350. GIDA, accessed November 27, 2019, https://www.gida-global.org/.

351. GO FAIR, *FAIR Principles,* accessed November 27, 2019, https://www.go-fair.org/fair-principles/.

352. David Heinemeier Hansson (@DHH), "The @AppleCard is such a fucking sexist program. My wife and I filed joint tax returns, live in a community-property state, and have been married for a long time. Yet Apple's black box algorithm thinks I deserve 20x the credit limit she does. No appeals work," Twitter, November 7, 2019, 12:34 p.m., https://twitter.com/dhh/status/1192540900393705474.

353. "Apple Co-Founder Steve Wozniak Says New Credit Card Discriminated Against His Wife," NBC News Now, uploaded November 12, 2019, YouTube video, 02:12, https://youtu.be/Htu6x4XhfQ0. See also Sarah Myers West, "In the Outcry over the Apple Card, Bias Is a Feature, Not a Bug," Medium, November 22, 2019,

https://medium.com/@AINowInstitute/in-the-outcry-over-the-apple-card-bias-is-a-feature-not-a-bug-532a4c75cc9f.

354. Sridhar Natarajan and Shahien Nasiripour, "Senator Wyden Says He's Looking into Claims of Apple Card Bias," *Bloomberg,* November 13, 2019: https://www.bloomberg.com/news/articles/2019-11-13/senator-wyden-says-he-s-looking-into-claims-of-apple-card-bias; Linda A. Lacewell, New York Department of Financial Services, "Building a Fairer and More Inclusive Financial Services Industry for Everyone," Medium, November 10, 2019, https://medium.com/@nydfs/building-a-fairer-and-more-inclusive-financial-services-industry-for-everyone-917183dae954.

355. See AI Now Institute, "Gender, Race, and Power in AI: A Playlist," Medium, April 17, 2019, https://medium.com/@AINowInstitute/gender-race-and-power-in-ai-a-playlist-2d3a44e43d3b; Joy Lisi Rankin, *A People's History of Computing in the United States* (Cambridge: Harvard University Press, 2018); Ruha Benjamin, *Race After Technology: Abolitionist Tools for the New Jim Code* (Medford, MA: Polity Press, 2019); Virginia Eubanks, *Automating Inequality: How High-Tech Tools Profile*, Police, and Punish the Poor (New York: St. Martin's Press, 2017); Mar Hicks, "Hacking the Cis-tem", *IEEE Annals of the History of Computing*, 41 no. 1 (Jan.-Mar 2019): 20-33. https://ieeexplore.ieee.org/document/8634814; Safiya Noble, *Algorithms of Oppression* (New York, NY: NYU Press, 2018).

356. Sarah Myers West, Meredith Whittaker, and Kate Crawford, "Discriminating Systems: Gender, Race, and Power in AI," AI Now Institute, April 2019, https://ainowinstitute.org/discriminatingsystems.pdf.

357. David Heinemeier Hansson (@DHH), Twitter, November 8, 2019, 2:08 p.m., https://twitter.com/dhh/status/1192926909794902016.

358. Marietje Schaake and Eric Schmidt, "Keynote: Regulating Big Tech," Stanford University HAI 2019 Fall Conference, uploaded on November 13, 2019, YouTube video, 1:18:25, https://youtu.be/uXpEYM0F5gA.

359. Microsoft Corporation, United States Securities and Exchange Commission Form 10-K: Annual Report for the Fiscal Year Ended June 30, 2019, retrieved November 27, 2019, https://view.officeapps.live.com/op/view.aspx?src=https://c.s-microsoft.com/en-us/CMSFiles/MSFT_FY19Q4_10K.docx?version=0a785912-1d8b-1ee0-f8d8-63f2fb7a5f00.

360. Myers West, Whittaker, and Crawford, "Discriminating Systems: Gender, Race, and Power in AI."

361. JF Gagne, "Global AI Talent Report 2019," retrieved November 27, 2019, https://jfgagne.ai/talent-2019/.

362. Yoav Shoam et al., "The AI Index 2018 Annual Report," AI Index Steering Committee, Human-Centered AI Initiative, Stanford University, December 2018, http://cdn.aiindex.org/2018/AI%20Index%202018%20Annual%20Report.pdf.

363. Myers West, Whittaker, and Crawford, "Discriminating Systems."

364. Jackie Snow, "'We're in a Diversity Crisis': Cofounder of Black in AI on What's Poisoning Algorithms in Our Lives," *MIT Technology Review*, February 14, 2018, https://www.technologyreview.com/s/610192/were-in-a-diversity-crisis-black-in-ais-founder-on-whats-poisoning-the-algorithms-in-our/.

365. Myers West, Whittaker, and Crawford, "Discriminating Systems." For a firsthand account, see EricaJoy, "#FFFFFF Diversity," Medium, October 7, 2015, https://medium.com/this-is-hard/ffffff-diversity-1bd2b3421e8a.

366. "Canada Refuses Visas to over a Dozen African AI Researchers," BBC News, November 15, 2019, https://www.bbc.com/news/world-us-canada-50426774; Kristian Lum, "Statistics, We Have a Problem,"

Medium, December 13, 2017,
https://medium.com/@kristianlum/statistics-we-have-a-problem-304638dc5de5.

367. Corinne Purtill, "A Nude 'Playboy' Photo Has Been a Mainstay in Testing Tech for Decades," *OneZero*, Medium, November 26, 2019:
https://onezero.medium.com/a-nude-playboy-photo-has-been-a-mainstay-in-testing-tech-for-decades-b8cdb434dce1.

368. Meredith Whittaker et al., "Disability, Bias, and AI," AI Now Institute, November 2019,
https://ainowinstitute.org/disabilitybiasai-2019.pdf.

369. Louise Matsakisis, "Thousands of Tech Workers Join Global Climate Change Strike," *Wired*, September 20, 2019, https://www.wired.com/story/tech-workers-global-climate-change-strike/.

370. Tech Workers Coalition, "There's a Climate Crisis and Tech Workers Are Walking Out," accessed November 22, 2019, https://techworkerscoalition.org/climate-strike/.

371. Roel Dobbe and Meredith Whittaker, "AI and Climate Change: How They're Connected, and What We Can Do about It," AI Now Institute, Medium, October 17, 2019,
https://medium.com/@AINowInstitute/ai-and-climate-change-how-theyre-connected-and-what-we-can-do-about-it-6aa8d0f5b32c.

372. Lotfi Belkhir and Ahmed Elmeligi, "Assessing ICT Global Emissions Footprint: Trends to 2040 & Recommendations," *Journal of Cleaner Production* 177 (March 10, 2018): 448–63,
https://doi.org/10.1016/j.jclepro.2017.12.239.

373. Air Transport Action Group. "Facts & Figures." Accessed November 22, 2019.
https://www.atag.org/facts-figures.html.

374. Wikipedia, s.v. "List of Countries by Greenhouse Gas Emissions," accessed November 13, 2019,
https://en.wikipedia.org/w/index.php?title=List_of_countries_by_greenhouse_gas_emissions&oldid=925976447.

375. Google Sustainability, "100% Renewable Is Just the Beginning," accessed November 22, 2019,
https://sustainability.google/projects/announcement-100; Microsoft, "AI for Earth," accessed October 18, 2019, https://www.microsoft.com/en-us/ai/ai-for-earth.

376. Belkhir and Elmeligi, "Assessing ICT Global Emissions Footprint: Trends to 2040 & Recommendations,"
https://doi.org/10.1016/j.jclepro.2017.12.239.

377. Gary Cook et al., "Clicking Clean: Who Is Winning the Race to Build a Green Internet?," Greenpeace, January 2017, http://www.clickclean.org/international/en/.

378. Mike Hazas, Janine Morley, Oliver Bates, and Adrian Friday, "Are There Limits to Growth in Data Traffic?: On Time Use, Data Generation and Speed," *Proceedings of the Second Workshop on Computing Within Limits* (2016) 14:1–14:5, https://doi.org/10.1145/2926676.2926690.

379. Energy Realpolitik, "What 5G Means for Energy," Council on Foreign Relations, accessed November 22, 2019, https://www.cfr.org/blog/what-5g-means-energy.

380. Mary-Ann Russon, "Will 5G Be Necessary for Self-Driving Cars?," BBC News, September 27, 2018,
https://www.bbc.com/news/business-45048264.

381. Anthony Cuthbertson, "Surgeon Performs World's First Remote Operation Using '5G Surgery' on Animal in China" *The Independent*, January 17, 2019,

https://www.independent.co.uk/life-style/gadgets-and-tech/news/5g-surgery-china-robotic-operation-a8732861.html.

382. Richard Sutton, "The Bitter Lesson," Incomplete Ideas (blog), March 13, 2019, http://www.incompleteideas.net/IncIdeas/BitterLesson.html.

383. Max Welling, "Do We Still Need Models or Just More Data and Compute?" University of Amsterdam, April 20, 2019, https://staff.fnwi.uva.nl/m.welling/wp-content/uploads/Model-versus-Data-AI.pdf.

384. Dario Amodei and Danny Hernandez, "AI and Compute," OpenAI (blog), May 16, 2018, https://openai.com/blog/ai-and-compute/.

385. Emma Strubell, Ananya Ganesh, and Andrew McCallum, "Energy and Policy Considerations for Deep Learning in NLP," *57th Annual Meeting of the Association for Computational Linguistics (ACL)*, Florence, Italy, July 2019, http://arxiv.org/abs/1906.02243.

386. Brian Merchant, "Amazon Is Aggressively Pursuing Big Oil as It Stalls Out on Clean Energy," *Gizmodo*, April 8, 2019, https://gizmodo.com/amazon-is-aggressively-pursuing-big-oil-as-it-stalls-ou-1833875828.

387. Cynthya Peranandam, "Your Guide to AI and Machine Learning at Re:Invent 2018," AWS Machine Learning Blog, September 27, 2018, https://aws.amazon.com/blogs/machine-learning/your-guide-to-ai-and-machine-learning-at-reinvent-2018/.

388. "Microsoft Demonstrates the Power of AI and Cloud to Oil and Gas Players, at ADIPEC 2018," Microsoft News Center, November 12, 2018, https://news.microsoft.com/en-xm/2018/11/12/microsoft-demonstrates-the-power-of-ai-and-cloud-to-oil-and-gas-players-at-adipec-2018/.

389. Google Cloud, "Infrastructure Modernization: Power Your Exploration and Production with High Performance Computing," accessed November 22, 2019, https://cloud.google.com/solutions/energy/.

390. "Baker Hughes, C3.ai, and Microsoft Announce Alliance to Accelerate Digital Transformation of the Energy Industry," BakerHughesC3.ai, November 19, 2019, https://bakerhughesc3.ai/baker-hughes-c3-ai-and-microsoft-announce-alliance-to-accelerate-digital-transformation-of-the-energy-industry/.

391. Zero Cool, "Oil Is the New Data," *Logic*, Issue 9, November 30, 2019. https://logicmag.io/nature/oil-is-the-new-data/.

392. Stephanie Kirchgaessner, "Revealed: Google Made Large Contributions to Climate Change Deniers," *Guardian*, October 11, 2019, https://amp.theguardian.com/environment/2019/oct/11/google-contributions-climate-change-deniers.

393. Belkhir and Elmeligi, "Assessing ICT Global Emissions Footprint: Trends to 2040 & Recommendations," https://doi.org/10.1016/j.jclepro.2017.12.239.

394. Cook et al., "Clicking Clean: Who Is Winning the Race to Build a Green Internet?," http://www.clickclean.org/international/en/.

395. Arvind Narayanan, "How to Recognize AI Snake Oil," Princeton University, Department of Computer Science, accessed November 20, 2019, https://www.cs.princeton.edu/~arvindn/talks/MIT-STS-AI-snakeoil.pdf.

396. Drew Harwell, "Rights Group Files Federal Complaint against AI-Hiring Firm HireVue, Citing 'Unfair and Deceptive' Practices," *Washington Post,* November 6, 2019,

https://www.washingtonpost.com/technology/2019/11/06/prominent-rights-group-files-federal-complaint-against-ai-hiring-firm-hirevue-citing-unfair-deceptive-practices/.

397. Clarice Smith, "Facial Recognition Enters into Healthcare," *Journal of AHIMA,* September 4, 2018, https://journal.ahima.org/2018/09/04/facial-recognition-enters-into-healthcare/.

398. Jane Li, "A 'Brain-Reading' Headband for Students Is Too Much Even for Chinese Parents," *Quartz,* November 5, 2019, https://qz.com/1742279/a-mind-reading-headband-is-facing-backlash-in-china/.

399. Paul Sawers, "Realeyes Raises $12.4 Million to Help Brands Detect Emotion Using AI on Facial Expressions," *VentureBeat,* June 6, 2019, https://venturebeat.com/2019/06/06/realeyes-raises-12-4-million-to-help-brands-detect-emotion-using-ai-on-facial-expressions/.

400. Luana Pascu, "New Kairos Facial Recognition Camera Offers Customer Insights," *Biometric Update,* September 11, 2019, https://www.biometricupdate.com/201909/new-kairos-facial-recognition-camera-offers-customer-insights.

401. Tom Simonite, "Amazon Says It Can Detect Fear on Your Face. Are You Scared?" *Wired,* August 18, 2019, https://www.wired.com/story/amazon-detect-fear-face-you-scared/.

402. Mike Butcher, "The Robot-Recruiter Is Coming — VCV's AI Will Read Your Face in a Job Interview," *TechCrunch,* April 23, 2019, https://techcrunch.com/2019/04/23/the-robot-recruiter-is-coming-vcvs-ai-will-read-your-face-in-a-job-interview/.

403. Tom Simonite, "This Call May Be Monitored for Tone and Emotion," *Wired,* March 19, 2019, https://www.wired.com/story/this-call-may-be-monitored-for-tone-and-emotion/; Kyle Wiggers, "Empath's AI Detects Emotion from Your Voice," *VentureBeat,* September 8, 2019, https://venturebeat.com/2019/09/08/empaths-ai-measures-emotion-from-voice/.

404. Cade Metz, "Google Glass May Have an Afterlife as a Device to Teach Autistic Child," *New York Times,* July 17, 2019, https://www.nytimes.com/2019/07/17/technology/google-glass-device-treat-autism.html.

405. BrainCo Inc., "Harvard University-Backed Startup BrainCo Inc. Gets the Biggest Purchase Order in Brain Machine Interface (BMI) Industry," *PR Newswire,* May 18, 2017, https://www.prnewswire.com/news-releases/harvard-university-backed-startup-brainco-inc-gets-the-biggest-purchase-order-in-brain-machine-interface-bmi-industry-300460485.html.

406. Andrew McStay, "Emotional AI and EdTech: Serving the Public Good?," *Learning, Media and Technology,* November 5, 2019, https://doi.org/10.1080/17439884.2020.1686016.

407. Mark Harris, "An Eye-Scanning Lie Detector Is Forging a Dystopian Future," *Wired*, April 12, 2019, https://www.wired.com/story/eye-scanning-lie-detector-polygraph-forging-a-dystopian-future/; and Amit Katwala, "The Race to Create a Perfect Lie Detector – and the Dangers of Succeeding," *Guardian,* September 5, 2019, https://www.theguardian.com/technology/2019/sep/05/the-race-to-create-a-perfect-lie-detector-and-the-dangers-of-succeeding.

408. "Detective 11.5," Oxygen Forensics, July 2019, https://www.oxygen-forensic.com/uploads/press_kit/OF_RN_11_5_web.pdf.

409. Jack Gillum and Jeff Kao, "Aggression Detectors: The Unproven, Invasive Surveillance Technology Schools Are Using to Monitor Students," *ProPublica*, June 25, 2019,

https://features.propublica.org/aggression-detector/the-unproven-invasive-surveillance-technology-schools-are-using-to-monitor-students/.

410. Lauren Rhue, "Racial Influence on Automated Perceptions of Emotions," November 9, 2018, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3281765.

411. Zhimin Chen and David Whitney, "Tracking the Affective State of Unseen Persons," *Proceedings of the National Academy of Sciences*, February 5, 2019, https://www.pnas.org/content/pnas/early/2019/02/26/1812250116.full.pdf.

412. Ruben Van De Ven, "Choose How You Feel; You Have Seven Options," Institute of Network Cultures, January 25, 2017, https://networkcultures.org/longform/2017/01/25/choose-how-you-feel-you-have-seven-options/.

413. Jayne Williamson-Lee, "Amazon's A.I. Emotion-Recognition Software Confuses Expressions for Feelings," *OneZero*, Medium, October 28, 2019, https://onezero.medium.com/amazons-a-i-emotion-recognition-software-confuses-expressions-for-feelings-53e96007ca63.

414. Lisa Feldman Barrett, Ralph Adochs, and Stacy Marsella, "Emotional Expressions Reconsidered: Challenges to Inferring Emotion From Human Facial Movements," *Psychological Science in the Public Interest* 20, no. 1 (July 2019): 1–68, https://journals.sagepub.com/eprint/SAUES8UM69EN8TSMUGF9/full.

415. Barrett et al., "Emotional Expressions Reconsidered."

416. Steve Lohr, "Facial Recognition Is Accurate If You're A White Guy," *New York Times*, February 9 2018, https://www.nytimes.com/2018/02/09/technology/facial-recognition-race-artificial-intelligence.html; and Natasha Singer, "Amazon Is Pushing Facial Technology That a Study Says Could Be Biased," *New York Times*, January 24, 2019, https://www.nytimes.com/2019/01/24/technology/amazon-facial-technology-study.html.

417. Cade Metz, "Facial Recognition Tech Is Growing Stronger, Thanks to Your Face," *New York Times*, July 13, 2019, https://www.nytimes.com/2019/07/13/technology/databases-faces-facial-recognition-technology.html.

418. See "Diversity in Faces Dataset," IBM, https://www.research.ibm.com/artificial-intelligence/trusted-ai/diversity-in-faces/; see also Michele Merler, Nalini Ratha, Rogerio Feris, and John R. Smith, "Diversity in faces," *arXiv:1901.10436*, January 29, 2019, https://arxiv.org/abs/1901.10436.

419. Bart Thomée and David A. Shamma, "The Ins and Outs of the Yahoo Flickr Creative Commons 100 Million Dataset," code.flickr.com, October 15, 2014, https://code.flickr.net/2014/10/15/the-ins-and-outs-of-the-yahoo-flickr-100-million-creative-commons-dataset/.

420. Olivia Solon, "Facial Recognition's 'Dirty Little Secret': Millions of Online Photos Scraped without Consent," NBC News, March 12, 2019, https://www.nbcnews.com/tech/internet/facial-recognition-s-dirty-little-secret-millions-online-photos-scraped-n981921.

421. Adam Harvey and Jules LaPlace, "MegaPixels: Origins, Ethics, and Privacy Implications of Publicly Available Face Recognition Image Datasets," April 18, 2019, https://megapixels.cc/about/.

422. Duke MTMC Dataset Analysis, 2016, https://megapixels.cc/datasets/duke_mtmc/.

423. Brainwash Dataset Analysis, 2015, https://megapixels.cc/datasets/brainwash/.

424. See, for example, Oxford Town Centre Dataset Analysis, 2009, https://megapixels.cc/datasets/oxford_town_centre/; and UnConstrained College Students Dataset Analysis, 2012–2013, https://megapixels.cc/datasets/uccs/.

425. Joy Buolamwini, "Response: Racial and Gender bias in Amazon Rekognition — Commercial AI System for Analyzing Faces," Medium, January 25, 2019, https://medium.com/@Joy.Buolamwini/response-racial-and-gender-bias-in-amazon-rekognition-commercial-ai-system-for-analyzing-faces-a289222eeced.

426. For a comprehensive look at the state of technology in healthcare, see Eric Topol, *Deep Medicine* (New York: Basic Books, 2019).

427. See, for example, "Artificial Intelligence for Health," ITU, https://aiforgood.itu.int/ai4health/#about. For a critical take on the "AI for good" narrative, see Mark Latonero, "AI for Good Is Often Bad," *Wired,* November 18, 2019, https://www.wired.com/story/opinion-ai-for-good-is-often-bad/.

428. Andrzej Grzybowski et al. "Artificial Intelligence for Diabetic Retinopathy Screening: A Review," *Eye*, September 5, 2019, https://doi.org/10.1038/s41433-019-0566-0.

429. Mason Marks, "Tech Companies Are Using AI to Mine Our Digital Traces," *STAT,* September 17, 2019, https://www.statnews.com/2019/09/17/digital-traces-tech-companies-artificial-intelligence/.

430. For infrastructural approaches to analyzing algorithms, see Jean-Christophe Plantin, Carl Lagoze, Paul N. Edwards, and Christian Sandvig, "Infrastructure Studies Meet Platform Studies in the Age of Google and Facebook," *New Media & Society* 20, no. 1 (January 2018): 293–310, https://doi.org/10.1177/1461444816661553; and Paul N. Edwards, "We Have Been Assimilated: Some Principles for Thinking About Algorithmic Systems," in *Living with Monsters? Social Implications of Algorithmic Phenomena, Hybrid Agency, and the Performativity of Technology: IFIP WG 8.2 Working Conference on the Interaction of Information Systems and the Organization, IS&O 2018, San Francisco, CA, USA, December 11–12, 2018, Proceedings*, eds. Ulrike Schultze, Margunn Aanestad, Magnus Mähring, Carsten Østerlund, Kai Riemer (Cham, Switzerland: Springer International Publishing, 2018).

431. Rob Copeland, "Google's 'Project Nightingale' Gathers Personal Health Data on Millions of Americans," *Wall Street Journal*, November 2019, https://www.wsj.com/articles/google-s-secret-project-nightingale-gathers-personal-health-data-on-millions-of-americans-11573496790; Anonymous, "I'm the Google Whistleblower. The Medical Data of Millions of Americans Is at Risk," *Guardian*, November 14, 2019, https://www.theguardian.com/commentisfree/2019/nov/14/im-the-google-whistleblower-the-medical-data-of-millions-of-americans-is-at-risk.

432. In the US Health Insurance Portability and Accountability Act (HIPAA), personal health information (PHI) is categorized as data that is directly and uniquely tied to an individual, with examples including names, birth dates, and email addresses.De-identified data, therefore, indicates the absence of such categories from a potential EHR dataset.

433. Tariq Shaukat, "Our Partnership with Ascension," Inside Google Cloud, November 11, 2019 (last modified November 12, 2019), https://cloud.google.com/blog/topics/inside-google-cloud/our-partnership-with-ascension.

434. The cloud computing market size for healthcare is anticipated to reach nearly $30 billion by 2026. Google, Amazon, and Microsoft have all partnered with healthcare providers and payers to help migrate health information technology (HIT) infrastructure to cloud servers. Amazon Web Services now promises clients the ability to subscribe to third-party data, enabling healthcare professionals to aggregate data from

clinical trials, while Microsoft has partnered with the insurance company Humana to provide cloud and AI resources, and also helps power Epic Systems' predictive analytics tools for EHRs.

435. Daisuke Wakabayashi, "Google and the University of Chicago Are Sued over Data Sharing, *New York Times*, June 26, 2019, https://www.nytimes.com/2019/06/26/technology/google-university-chicago-data-sharing-lawsuit.html; Rebecca Robbins and Casey Ross, "HSS to Probe Whether Project Nightingale Followed Privacy Law," *STAT*, November 13, 2019, https://www.statnews.com/2019/11/13/hhs-probe-google-ascension-project-nightingale/; Timothy Revell, "Google DeepMind NHS Data Deal Was 'Legally Inappropriate'," *New Scientist*, May 16, 2017, https://www.newscientist.com/article/2131256-google-deepmind-nhs-data-deal-was-legally-inappropriate/.

436. Boris P. Hejblum et al, "Probabilistic Record Linkage of De-identified Research Datasets with Discrepancies Using Diagnosis Codes," *Scientific Data* 6, 180298 (January 2019), https://doi.org/10.1038/sdata.2018.298.

437. Gina Kolata, "You Got a Brain Scan at the Hospital. Someday a Computer May Use It to Identify You," *New York Times,* October 23, 2019, https://www.nytimes.com/2019/10/23/health/brain-scans-personal-identity.html.

438. *Dinerstein v. Google, LLC*, https://edelson.com/wp-content/uploads/2016/05/Dinerstein-Google-DKT-001-Complaint.pdf.

439. Gyeongcheol Cho, Jinyeong Yim, Younyoung Choi, Jungmin Ko, and Seoung-Hwan Lee, "Review of Machine Learning Algorithms for Diagnosing Mental Illness," *Psychiatry Investigation* 16, no. 4 (April 2019): 262–69, https://doi.org/10.30773/pi.2018.12.21.2. For ethical concerns, see Mason Marks, "Artificial Intelligence Based Suicide Prediction," *Yale Journal of Health Policy, Law, and Ethics* (forthcoming, 2019), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3324874; and Stevie Chancellor et al., "A Taxonomy of Ethical Tensions in Inferring Mental Health States from Social Media," *Proceedings of the Conference on Fairness, Accountability, and Transparency*, FAT* '19 (2019): 79–88, https://doi.org/10.1145/3287560.3287587.

440. Recent examples include Irene Y. Chen, Peter Szolovits, and Marzyeh Ghassemi, "Can AI Help Reduce Disparities in General Medical and Mental Health Care?," *AMA Journal of Ethics* 21, no. 2 (February 1, 2019): 167–79, https://doi.org/10.1001/amajethics.2019.167; Jessica Morley and Luciano Floridi, "How to Design a Governable Digital Health Ecosystem," July 22, 2019, https://dx.doi.org/10.2139/ssrn.3424376; Linda Nordling, "A Fairer Way Forward for AI in Health Care," *Nature* 573 (September 25, 2019): S103–5, https://doi.org/10.1038/d41586-019-02872-2; Trishan Panch, Heather Mattie, and Leo Anthony Celi, "The 'Inconvenient Truth' about AI in Healthcare," *npj Digital Medicine* 2, no. 1 (August 16, 2019): 1–3, https://doi.org/10.1038/s41746-019-0155-4.

441. J. Raymond Geis et al., "Ethics of Artificial Intelligence in Radiology: Summary of the Joint European and North American Multisociety Statement," *Radiology*, 293, no.2 (October 2019), https://doi.org/10.1148/radiol.2019191586.

442. Geis et al., 3.

443. Geis et al., 4.

444. Geis et al., 12.

445. Academy of Medical Royal Colleges, "Artificial Intelligence in Healthcare," January 2019, https://www.aomrc.org.uk/wp-content/uploads/2019/01/Artificial_intelligence_in_healthcare_0119.pdf.

446. American Medical Association, "Augmented intelligence in healthcare H-480.940," last modified 2018, accessed November 21, 2019,

https://policysearch.ama-assn.org/policyfinder/detail/augmented%20intelligence?uri=%2FAMADoc%2FHOD.xml-H-480.940.xml; Elliott Crigger and Christopher Khoury, "Making Policy on Augmented Intelligence in Health Care," *AMA J Ethics* 21, no.2 (February 2019): E188–191, https://doi.org/10.1001/amajethics.2019.188.

447. Eric Topol, "Why Doctors Should Organize," *New Yorker*, August 5, 2019, https://www.newyorker.com/culture/annals-of-inquiry/why-doctors-should-organize.

448. Topol, "Why Doctors Should Organize."

449. Angela Lashbrook, "AI-Driven Dermatology Could Leave Dark-Skinned Patients Behind," *Atlantic*, August 16, 2018, https://www.theatlantic.com/health/archive/2018/08/machine-learning-dermatology-skin-color/567619/.

450. Dhruv Khullar, "A.I. Could Worsen Health Disparities," *The New York Times*, January 31, 2019, https://www.nytimes.com/2019/01/31/opinion/ai-bias-healthcare.html.

451. Carolyn Y. Johnson, "Racial Bias in a Medical Algorithm Favors White Patients over Sicker Black Patients," *Washington Post*, October 24, 2019, https://www.washingtonpost.com/health/2019/10/24/racial-bias-medical-algorithm-favors-white-patients-over-sicker-black-patients/. For original article, see Ziad Obermeyer, Brian Powers, Christine Vogeli, and Sendhil Mullainathan, "Dissecting Racial Bias in an Algorithm Used to Manage the Health of Populations," *Science* 366, no. 6464 (October 2019): 447–453.

452. For examples of how technology design can impact health inequities, see Tiffany C. Veinot, Hannah Mitchell, Jessica S. Ancker, "Good Intentions Are Not Enough: How Informatics Interventions Can Worsen Inequality," *Journal of the American Medical Informatics Association* 25, no. 8 (August 2018): 1080–1088, https://doi.org/10.1093/jamia/ocy052; Elizabeth Kaziunas, Michael S. Klinkman, and Mark S. Ackerman, "Precarious Interventions: Designing for Ecologies of Care," *Proceedings of the ACM Human-Computer Interaction* 3, CSCW, Article 113 (November 2019), https://doi.org/10.1145/3359215.

453. "AI Now Report 2018," https://ainowinstitute.org/AI_Now_2018_Report.pdf. See Section 2.1.

454. Julia Powles and Helen Nissenbaum, "The Seductive Diversion of 'Solving' Bias in Artificial Intelligence," *One Zero*, Medium, December 7, 2018, https://onezero.medium.com/the-seductive-diversion-of-solving-bias-in-artificial-intelligence-890df5e5ef53.

455. Andrew D. Selbst, danah boyd, Sorelle Friedler, Suresh Venkatasubramanian, and Janet Vertesi, "Fairness and Abstraction in Sociotechnical Systems," November 7, 2018, https://papers.ssrn.com/abstract=3265913.

456. Samir Passi and Solon Barocas, "Problem Formulation and Fairness," *Proceedings of the Conference on Fairness, Accountability, and Transparency*, FAT* '19 (2019), 39–48, https://doi.org/10.1145/3287560.3287567.

457. Anna Lauren Hoffman, "Where Fairness Fails: Data, Algorithms, and the Limits of Antidiscrimination Discourse," *Information, Communication & Society* 22, no. 7 (June 7, 2019): 900–915, https://doi.org/10.1080/1369118X.2019.1573912.

458. Issa Kohler-Hausmann. "Eddie Murphy and the Dangers of Counterfactual Causal Thinking About Detecting Racial Discrimination," January 1, 2019, https://papers.ssrn.com/abstract=3050650.

459. Lily Hu, "Disparate Causes, Pt. II," Phenomenal World (blog), October 17, 2019, https://phenomenalworld.org/digital-ethics/disparate-causes-pt-ii.

460. Christopher Jung, Michael Kearns, Seth Neel, Aaron Roth, Logan Stapleton, and Zhiwei Steven Wu, "Eliciting and Enforcing Subjective Individual Fairness," *arXiv:1905.10660 [cs.LG]*, (2019), https://arxiv.org/abs/1905.10660.

461. Hoffmann, "Where Fairness Fails," https://doi.org/10.1080/1369118X.2019.1573912.

462. Ann-Kathrin Dombrowski, Maximilian Alber, Christopher J. Anders, Marcel Ackermann, Klaus-Robert Müller, and Pan Kessel, "Explanations Can Be Manipulated and Geometry Is to Blame," *arXiv:1906.07983 [Cs, Stat]*, September 25, 2019, http://arxiv.org/abs/1906.07983; Amirata Ghorbani, Abubakar Abid, and James Zou, "Interpretation of Neural Networks Is Fragile," *arXiv:1710.10547 [Cs, Stat]*, November 6, 2018, http://arxiv.org/abs/1710.10547; Akshayvarun Subramanya, Vipin Pillai, and Hamed Pirsiavash, "Fooling Network Interpretation in Image Classification," *arXiv:1812.02843 [Cs]*, September 24, 2019, http://arxiv.org/abs/1812.02843.

463. Tim Miller, "Explanation in Artificial Intelligence: Insights from the Social Sciences," *Artificial Intelligence* 267 (2019): 1–38, https://arxiv.org/abs/1706.07269.

464. See, for example, the ACM FAT* conference, https://fatconference.org/2020/callforcraft.html.

465. Roel Dobbe and Morgan G. Ames, "Translation Tutorial: Values, Engagement and Reflection in Automated Decision Systems," presented at the ACM Conference on Fairness, Accountability, and Transparency, Atlanta, January 2019; see also Dobbe and Ames, "Up Next For FAT*: From Ethical Values To Ethical Practices," Medium, February 8, 2019, https://medium.com/@roeldobbe/up-next-for-fat-from-ethical-values-to-ethical-practices-ebbed9f6adee.

466. Margaret Mitchell, Simone Wu, Andrew Zaldivar, Parker Barnes, Lucy Vasserman, Ben Hutchinson, Elena Spitzer, Inioluwa Deborah Raji, and Timnit Gebru, "Model Cards for Model Reporting," *Proceedings of the Conference on Fairness, Accountability, and Transparency*, FAT* '19 (2019): 220–229, https://doi.org/10.1145/3287560.3287596; Timnit Gebru, Jamie Morgenstern, Briana Vecchione, Jennifer Wortman Vaughan, Hanna Wallach, Hal Daumeé III, and Kate Crawford, "Datasheets for Datasets," *arXiv:1803.09010* (2018), https://arxiv.org/abs/1803.09010?context=cs; Matthew Arnold, Rachel KE Bellamy, Michael Hind, Stephanie Houde, Sameep Mehta, Aleksandra Mojsilovic, Ravi Nair, et al., "FactSheets: Increasing Trust in AI Services through Supplier's Declarations of Conformity," *IBM Journal of Research and Development* (2019), https://arxiv.org/pdf/1808.07261.pdf.

467. Partnership on AI, "About ML: Annotation and Benchmarking on Understanding and Transparency of Machine Learning Lifecycles," https://www.partnershiponai.org/about-ml/; Ethics in Action, IEEE, https://ethicsinaction.ieee.org.

468. Benjamin Wilson, Judy Hoffman, and Jamie Morgenstern, "Predictive Inequity in Object Detection," *arXiv:1902.11097*, February 21, 2019, https://arxiv.org/pdf/1902.11097.pdf.

469. Mahmoudreza Babaei, Abhijnan Chakraborty, Juhi Kulshrestha, Elissa M. Redmiles, Meeyoung Cha, and Krishna P. Gummadi, "Analyzing Biases in Perception of Truth in News Stories and Their Implications for Fact Checking," *Proceedings of the Conference on Fairness, Accountability, and Transparency*, FAT* '19 (2019): 139, https://dl.acm.org/citation.cfm?id=3287581.

470. Terrance de Vries, Ishan Misra, Changhan Wang, and Laurens van der Maaten, "Does Object Recognition Work for Everyone?," *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops* (2019): 52–59, https://research.fb.com/wp-content/uploads/2019/06/Does-Object-Recognition-Work-for-Everyone.pdf.

471. Ziad Obermeyer and Sendhil Mullainathan, "Dissecting Racial Bias in an Algorithm that Guides Health Decisions for 70 Million People," *Proceedings of the Conference on Fairness, Accountability, and Transparency*, FAT* '19 (2019): 89–89, https://dl.acm.org/citation.cfm?id=3287593.

472. Ruth Reader, "Technology Biased against Black Patients Runs Rampant in Hospitals," *Fast Company*, October 28, 2019, https://www.fastcompany.com/90422523/biased-technology-that-favors-white-patients-runs-rampant-in-hospitals.

473. Inioluwa Deborah Raji and Joy Buolamwini, "Actionable Auditing: Investigating the Impact of Publicly Naming Biased Performance Results of Commercial AI Products," *Proceedings of the 2019 AAAI/ACM Conference on AI, Ethics, and Society*, (2019): 429–435, https://doi.org/10.1145/3306618.3314244.

474. Raji and Buolamwini, "Actionable Auditing: Investigating the Impact of Publicly Naming Biased Performance Results of Commercial AI Products," https://doi.org/10.1145/3306618.3314244; Obermeyer and Mullainathan, "Dissecting Racial Bias in an Algorithm that Guides Health Decisions for 70 Million People," https://dl.acm.org/citation.cfm?id=3287593.

475. Dina Bass, "Amazon Schooled on AI Facial Technology By Turing Award Winner," *Bloomberg*, April 3 2019, https://www.bloomberg.com/news/articles/2019-04-03/amazon-schooled-on-ai-facial-technology-by-turing-award-winner.

476. Joy Buolamwini and Timnit Gebru, "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification," Conference on Fairness, Accountability and Transparency (2018): 77–91, http://gendershades.org/. Raji and Buolamwini, "Actionable Auditing: Investigating the Impact of Publicly Naming Biased Performance Results of Commercial AI Products," https://doi.org/10.1145/3306618.3314244.

477. Tom Simonite, "The Best Algorithms Struggle to Recognize Black Faces Equally," *Wired*, July 22, 2019, https://www.wired.com/story/best-algorithms-struggle-recognize-black-faces-equally/; James Vincent, "The Tech Industry Doesn't Have a Plan for Dealing with Bias in Facial Recognition," *The Verge*, July 26, 2019, https://www.theverge.com/2018/7/26/17616290/facial-recognition-ai-bias-benchmark-test.

478. Kushal Vangara, Michael C. King, Vitor Albiero, and Kevin Bowyer, "Characterizing the Variability in Face Recognition Accuracy Relative to Race," *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops*, April 15, 2019, https://arxiv.org/abs/1904.07325v3.

479. Jacob Snow, "Amazon's Face Recognition Falsely Matched 28 Members of Congress With Mugshots," ACLU, July 26, 2019, https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazons-face-recognition-falsely-matched-28.

480. Kate Gill, "Amazon Facial Recognition Falsely Links 27 Athletes to Mugshots in ACLU Study," *Hyperallergic*, October 28, 2019, https://hyperallergic.com/525209/amazon-facial-recognition-aclu/.

481. Blaine Nelson, Marco Barreno, Fuching Jack Chi, Anthony D. Joseph, Benjamin IP Rubinstein, Udam Saini, Charles A. Sutton, J. Doug Tygar, and Kai Xia, "Exploiting Machine Learning to Subvert Your Spam Filter," *LEET '08 Proceedings of the 1st Usenix Workshop on Large-Scale Exploits and Emergent Threats*, April 15, 2008, https://www.usenix.org/conference/leet-08/exploiting-machine-learning-subvert-your-spam-filter. More recently, examples of poisoning were reported for modifying explainability methods, attacking text generators, and bypassing plagiarism and copyright detectors. See Dombrowski et al., "Explanations Can Be Manipulated and Geometry Is to Blame," http://arxiv.org/abs/1906.07983; Dylan Slack, Sophie Hilgard, Emily Jia, Sameer Singh, and Himabindu Lakkaraju, "How Can We Fool LIME and SHAP? Adversarial Attacks on Post Hoc Explanation Methods," *arXiv:1911.02508 [Cs, Stat]*, November 6, 2019, http://arxiv.org/abs/1911.02508; Eric Wallace, Shi Feng, Nikhil Kandpal, Matt Gardner, and Sameer Singh, "Universal Adversarial Triggers for Attacking and Analyzing NLP," *arXiv:1908.07125 [Cs]*, August 29, 2019, http://arxiv.org/abs/1908.07125; Parsa Saadatpanah, Ali Shafahi, and Tom Goldstein, "Adversarial Attacks

on Copyright Detection Systems," *arXiv:1906.07153 [Cs, Stat]*, June 20, 2019, http://arxiv.org/abs/1906.07153.

482. Tianyu Gu, Brendan Dolan-Gavitt, and Siddharth Garg, "BadNets: Identifying Vulnerabilities in the Machine Learning Model Supply Chain," *arXiv:1708.06733 [Cs]*, March 11, 2019, http://arxiv.org/abs/1708.06733.

483. Srivatsan Srinivasan, "Artificial Intelligence, Cloud, Data Trends for 2019 and Beyond," Medium, March 12, 2019, https://medium.com/datadriveninvestor/artificial-intelligence-cloud-data-trends-for-2019-and-beyond-2cbdd9e54c36.

484. Sebastian Ruder, Matthew E. Peters, Swabha Swayamdipta, and Thomas Wolf, "Transfer Learning in Natural Language Processing," *Proceedings of the 2019 Conference of the North American Chapter of the Association for Computational Linguistics: Tutorials*, June 2019, https://doi.org/10.18653/v1/N19-5004.

485. Pedro Marcelino, "Transfer Learning from Pre-Trained Models," *Towards Data Science*, Medium, October 23, 2018, https://towardsdatascience.com/transfer-learning-from-pre-trained-models-f2393f124751.

486. Bolun Wang, Yuanshun Yao, Bimal Viswanath, Haitao Zheng, and Ben Y. Zhao, "With Great Training Comes Great Vulnerability: Practical Attacks against Transfer Learning," *27th USENIX Security Symposium*, August 2018, https://www.usenix.org/system/files/conference/usenixsecurity18/sec18-wang.pdf; Todor Davchev, Timos Korres, Stathi Fotiadis, Nick Antonopoulos, and Subramanian Ramamoorthy, "An Empirical Evaluation of Adversarial Robustness under Transfer Learning," *arXiv:1905.02675 [Cs, Stat]*, June 8, 2019, http://arxiv.org/abs/1905.02675.

487. Nicholas Carlini and David Wagner, "Towards Evaluating the Robustness of Neural Networks," *arXiv:1608.04644v2 [cs.CR]*, August 16, 2016, https://arxiv.org/abs/1608.04644v2.

488. Samuel G. Finlayson, John D. Bowers, Joichi Ito, Jonathan L. Zittrain, Andrew L. Beam, and Isaac S. Kohane, "Adversarial Attacks on Medical Machine Learning." *Science* 363, no. 6433 (March 22, 2019): 1287–89, https://doi.org/10.1126/science.aaw4399.

489. Nicholas Carlini, Anish Athalye, Nicolas Papernot, Wieland Brendel, Jonas Rauber, Dimitris Tsipras, Ian Goodfellow, and Aleksander Madry, "On Evaluating Adversarial Robustness," *arXiv:1902.06705v2 [cs.LG]*, February 18, 2019, https://arxiv.org/abs/1902.06705v2.

490. Whittaker et al., "AI Now Report 2018," https://ainowinstitute.org/AI_Now_2018_Report.pdf.

491. E. Gabriella Coleman, *Coding Freedom: The Ethics and Aesthetics of Hacking* (Princeton: Princeton University Press, 2013); E. Gabriella Coleman and Alex Golub, "Hacker Practice: Moral Genres and the Cultural Articulation of Liberalism," *Anthropological Theory* 8, no. 3 (September 2008): 255–77, https://doi.org/10.1177/1463499608093814; Kevin D. Mitnick, William L. Simon, and Steve Wozniak, *The Art of Deception: Controlling the Human Element of Security* (Indianapolis: Wiley, 2003).

492. Elda Paja, Fabiano Dalpiaz, and Paolo Giorgini, "Modelling and Reasoning about Security Requirements in Socio-Technical Systems," *Data & Knowledge Engineering* 98 (2015): 123–143; Matt Goerzen, Elizabeth Anne Watkins, and Gabrielle Lim, "Entanglements and Exploits: Sociotechnical Security as an Analytic Framework," 2019, https://www.usenix.org/conference/foci19/presentation/goerzen.

493. Ben Green and Salomé Viljoen, "Algorithmic Realism: Expanding the Boundaries of Algorithmic Thought," *Proceedings of the ACM Conference on Fairness, Accountability, and Transparency (FAT*)*, 2020.

494. Roel Dobbe, Thomas Gilbert, and Yonatan Mintz, "Hard Choices in Artificial Intelligence: Addressing Normative Uncertainty Through Sociotechnical Commitments," Neurips 2019 Workshop on AI for Social Good, *arXiv:1911.09005v1 [cs.AI]*, November 20, 2019, https://arxiv.org/abs/1911.09005v1.