AI NOW

2023 LANDSCAPE

# CONFRONTING TECH POWER

Our latest annual report diagnoses concentration of power in the tech industry as a pressing challenge - and points the path forward to seize this moment of change.

## ACKNOWLEDGEMENTS

Authored by Amba Kak and Dr. Sarah Myers West.

With research and editorial contributions from Alejandro Calcaño, Jane Chung, Dr. Kerry McInerney and Meredith Whittaker.

Copyediting by Caren Litherland.

Design by Partner & Partners.

Special thanks to all those that provided feedback on sections in the report including Veena Dubal, Ryan Gerety, Sara Geoghegan, Ellen Goodman, Alex Harman, Daniel Leufer, Estelle Masse, Fanny Hidvegi, Tamara Kneese, J. Nathan Mathias, Julia Powles, Daniel Rangel, Gabrielle Rejouis, Maurice Stucke, Charlotte Slaiman, Lori Wallach, Ben Winters, and Jai Vipra.

Cite as: Amba Kak and Sarah Myers West, “AI Now 2023 Landscape: Confronting Tech Power”, AI Now Institute, April 11, 2023, https://ainowinstitute.org/2023-landscape.

# Table of Contents

# Executive Summary

Artificial intelligence[1] is captivating our attention, generating both fear and awe about what's coming next. As increasingly dire prognoses about AI's future trajectory take center stage in the headlines about generative AI, it's time for regulators, and the public, to ensure that there is nothing about artificial intelligence (and the industry that powers it) that we need to accept as given. This watershed moment must also swiftly give way to action: to galvanize the considerable energy that has already accumulated over several years towards developing meaningful checks on the trajectory of AI technologies. This must start with confronting the concentration of power in the tech industry.

The AI Now Institute was founded in 2017, and even within that short span we've witnessed similar hype cycles wax and wane: when we wrote the 2018 AI Now report, the proliferation of facial recognition systems already seemed well underway, until pushback from local communities pressured government officials to pass bans in cities across the United States and around the world.[2] Tech firms were associated with the pursuit of broadly beneficial innovation,[3] until worker-led organizing, media investigations, and advocacy groups shed light on the many dimensions of tech-driven harm.[4]

These are only a handful of examples, and what they make clear is that **there is nothing about artificial intelligence that is inevitable.** Only once we stop seeing AI as synonymous with progress can we establish popular control over the trajectory of these technologies and meaningfully confront their serious social, economic, and political impacts—from exacerbating patterns of inequality in housing,[5] credit,[6] healthcare,[7] and education[8] to inhibiting workers' ability to organize[9] and incentivizing content production that is deleterious to young people's mental and physical health.[10]

In 2021, several members of AI Now were asked to join the Federal Trade Commission (FTC) to advise the Chair's office on artificial intelligence.[11] This was, among other things, a recognition of the growing centrality of AI to digital markets and the need for regulators to pay close attention to potential harms

[1] The term 'artificial intelligence' has come to mean many different things over the course of its history, and may be best understood as a marketing term rather than a fixed object. See for example: Michael Atleson, "Keep your AI Claims in Check", Federal Trade Commission, February 27, 2023,; Meredith Whittaker, "Signal, and the Tech Business Model Shaping Our World", Conference on Steward-Ownership 2023,, Annie Lowery, "AI Isn't Omnipotent. It's Janky", The Atlantic, April 3, 2023.

[2] Meredith Whittaker, Kate Crawford, Roel Dobbe, Genevieve Fried, Elizabeth Kaziunas, Varoon Mathur, Sarah Myers West, Rashida Richardson, Jason Schultz, Oscar Schwartz, *AI Now 2018 Report*, AI Now Institute, December 2018.
Tom Simonite, "Face Recognition Is Being Banned—But It's Still Everywhere," *Wired*, December 22, 2021.

[3] See Jenna Wortham, "Obama Brought Silicon Valley to Washington," New York Times, October 25, 2016,; and Cecilia Kang and Juliet Eilperin, "Why Silicon Valley Is the New Revolving Door for Obama Staffers," Washington Post, February 28, 2015.

[4] Varoon Mathur, Genevieve Fried, and Meredith Whittaker, "AI in 2019: A Year in Review," Medium , October 9, 2019.

[5] Robert Bartlett, Adair Morse, Richard Stanton, and Nancy Wallace, "Consumer-Lending Discrimination in the FinTech Era," *Journal of Financial Economics* 143, no. 1 (January 1, 2022): 30–56.

[6] Christopher Gilliard. "Prepared Testimony and Statement for the Record," Hearing on "Banking on Your Data: The Role of Big Data in Financial Services," House Financial Services Committee Task Force on Financial Technology, 2019.

[7] 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 25, 2019): 447–53.

[8] Rashida Richardson and Marci Lerner Miller, "The Higher Education Industry Is Embracing Predatory and Discriminatory Student Data Practices," *Slate*, January 13, 2021.

[9] Ibid.

[10] See Zach Praiss, "New Poll Shows Dangers of Social Media Design for Young Americans, Sparks Renewed Call for Tech Regulation," Accountable Tech, March 29, 2023; and Tawnell D. Hobbs, Rob Barry, and Yoree Koh, "'The Corpse Bride Diet': How TikTok Inundates Teens with Eating-Disorder Videos," *Wall Street Journal*, December 17, 2021.

[11] Federal Trade Commission, "FTC Chair Lina M. Khan Announces New Appointments in Agency Leadership Positions," press release, November 19, 2021.

to consumers and competition. Our experience within the US government helped clarify the path for the work ahead.

ChatGPT was unveiled during the last month of our time at the FTC, unleashing a wave of AI hype that shows no signs of letting up. This underscored the importance of addressing AI's role and impact, not as a philosophical futurist exercise but as something that is being used to shape the world around us here and now. We urgently need to be learning from the "move fast and break things" era of Big Tech; we can't allow companies to use our lives, livelihoods, and institutions as testing grounds for novel technological approaches, experimenting in the wild to our detriment. Happily, we do not need to draft policy from scratch: artificial intelligence, the companies that produce it, and the affordances required to develop these technologies already exist in a regulated space, and companies need to follow the laws already in effect. This provides a foundation, but we'll need to construct new tools and approaches, built on what we already have.

There is something different about this particular moment: it is primed for action. We have abundant research and reporting that clearly documents the problems with AI and the companies behind it. This means that more than ever before, we are prepared to **move from identifying and diagnosing harms to taking action to remediate them.** This will not be easy, but now is the moment for this work. This report is written with this task in mind: we are drawing from our experiences inside and outside government to outline an agenda for how we—as a group of individuals, communities, and institutions deeply concerned about the impact of AI unfolding around us—can meaningfully confront the core problem that AI presents, and one of the most difficult challenges of our time: **the concentration of economic and political power in the hands of the tech industry—Big Tech in particular.**

## There is no AI without Big Tech.

Over the past several decades, a handful of private actors have accrued power and resources that rival nation-states while developing and evangelizing artificial intelligence as critical social infrastructure. AI is being used to make decisions that shape the trajectory of our lives, from the deeply impactful, like what kind of job we get and how much we're paid; whether we can access decent healthcare and a good education; to the very mundane, like the cost of goods on the grocery shelf and whether the route we take home will send us into traffic.

Across all of these domains, the same problems show themselves: the technology doesn't work as claimed, and it produces high rates of error or unfair and discriminatory results. But the visible problems are only the tip of the iceberg. The opacity of this technology means we may not be informed when AI is in use, or how it's working. This ensures that we have little to no say about its impact on our lives.

**This is underscored by a core attribute of artificial intelligence: it is foundationally reliant on resources that are owned and controlled by only a handful of Big Tech firms.**

The dominance of Big Tech in artificial intelligence plays out along three key dimensions:

1. **The Data Advantage:** Firms that have access to the widest and deepest swath of behavioral data insights through surveillance will have an edge in the creation of consumer AI products. This is reflected in the acquisition strategies adopted by tech companies, which have of late focused on expanding this data advantage. Tech companies have amassed a tremendous degree of economic power, which has enabled them to embed themselves as core infrastructure within a number of industries, from health to consumer goods to education to credit.

2. **Computing Power Advantage:** AI is fundamentally a data-driven enterprise that is heavily reliant on substantial computing power to train, tune, and deploy these models. This is expensive and runs up against material dependencies such as chips and the location of data centers that mean efficiencies of scale apply, as well as labor dependencies on a relatively small pool of highly skilled tech workers that can most efficiently use these resources.[12] Only a handful of companies actually run their own infrastructure – the cloud and compute resources foundational to building AI systems. What this means is that even though "AI startups" abound, they must be understood as barnacles on the hull of Big Tech – licensing server infrastructure, and as a rule competing with each other to be acquired by one or another Big Tech firm. We are already seeing these firms wield their control over necessary resources to throttle competition. For example, Microsoft recently began penalizing customers for developing potential competitors to GPT-4, threatening to restrict their access to Bing search data.[13]

3. **Geopolitical Advantage:** AI systems (and the companies that produce them) are being recast not just as commercial products but foremost as strategic economic and security assets for the nation that need to be boosted by policy, and never restrained. The rhetoric around the US-China AI race has evolved from a sporadic talking point to an increasingly institutionalized stance (represented by collaborative initiatives between government, military, and Big Tech companies) that positions AI companies as crucial levers within this geopolitical fight. This narrative conflates the continued dominance of Big Tech as synonymous with US economic prowess, and ensures the continued accrual of resources and political capital to these companies.

To understand how we got here, we need to look at how tech firms presented themselves in their incipiency: their rise was characterized by marketing rhetoric promising that commercial tech would serve the public interest, encoding democratic values like freedom, democracy, and progress. But what's clear now is that the companies developing and deploying AI and related technologies are motivated by the same things that—structurally and necessarily—motivate all corporations: growth, profit, and rosy market valuations. This has been true from the start.

[12] For example, Microsoft is even rationing access to server hardware internally for some of its AI teams to ensure it has the capacity to run GPT-4. See Aaron Holmes and Kevin McLaughlin, "Microsoft Rations Access to AI Hardware for Internal Teams," *The Information*.

[13] Leah Nylen and Dina Bass, "Microsoft Threatens to Restrict Data in Rival AI Search," March 24, 2023.

## Why "Big Tech"?

In this report, we pay special attention to policy interventions that target large tech companies. The term "Big Tech" became popular around 2013[14] as a way to describe a handful of US-based megacorporations, and while it doesn't have a definite composition, today it's typically used as shorthand for Google, Apple, Facebook, Amazon, and Microsoft (often abbreviated as GAFAM), and sometimes also includes companies like Uber or Twitter.

It's a term that draws attention to the unique scale at which these companies operate: the network effects, data, and infrastructural advantages they have amassed. Big Tech's financial leverage has allowed these firms to consolidate this advantage across sectors from social media to healthcare to education and across media (like the recent pivot to virtual and augmented realities), often through strategic acquisitions. They seek to protect this advantage from regulatory threats through lobbying and similar non-capital strategies that leverage their deep pockets.[15] Following on from narratives around "Big Tobacco," "Big Pharma," and "Big Oil," this framing draws upon lessons from other domains where consolidation of power in industries has led to movements to reassert public accountability. (As one commentator puts it, "society does not prepend the label 'Big' with a capital B to an industry out of respect or admiration. It does so out of loathing and fear – and in preparation for battle."[16]) Recent name changes, like Google to Alphabet or Facebook to Meta, also make Big Tech helpful terminology to capture the sprawl of these companies and their continually shifting contours.[17]

Focusing on Big Tech is a useful prioritization exercise for tech policy interventions for several reasons:

- **Tackling challenges that either originate from or are exemplified by Big Tech companies can address the root cause of several key concerns:** invasive data surveillance, the manipulation of individual and collective autonomy, the consolidation of economic power, and exacerbation of patterns of inequality and discrimination, to name a few.

- **The Big Tech business and regulatory playbook has a range of knock-on effects on the broader ecosystem, incentivizing and even compelling other companies to fall in line.** Google and Facebook's adoption of the behavioral advertising business model that effectively propelled commercial surveillance into becoming the business model of the internet is just one example of this.

[14] Nick Dyer-Witheford and Alessandra Mularoni, "Framing Big Tech: News Media, Digital Capital and the Antitrust Movement," *Political Economy of Communication* 9, no. 2 (2021): 2–20.
[15] Zephyr Teachout and Lina Khan, "Market Structure and Political Law: A Taxonomy of Power," *Duke Journal of Constitutional Law & Public Policy* 9, no. 1 (2014): 37–74.
[16] Will Oremus, "Big Tobacco. Big Pharma. Big Tech?" *Slate*, November 17, 2017.
[17] Kean Birch Kean and Kelly Bronson, "Big Tech," *Science as Culture* 31, no. 1 (January 2, 2022): 1–14.

- **Growing dependencies on Big Tech across the tech industry and government make them a single point of failure.** A core business strategy for these firms is to make themselves infrastructural, and much of the wider tech ecosystem relies on them in one way or another, from cloud computing to advertising ecosystems and, increasingly, to payments. This makes these companies both a choke point and a single point of failure. We're also seeing spillover into the public sector. While a whole spectrum of vendors for AI and tech products sells to government agencies, the dependence of government on Big Tech affordances came into particular focus during the height of the pandemic, when many national governments needed to rely on Big Tech infrastructure, networks, and platforms for basic governance functions.

**Finally, this report takes aim not just at the pathologies associated with these companies, but also at the broader narratives that justify and normalize them.** From unrestricted innovation as a social good to digitization, to data as the only way to see and interpret the world, to platformization as necessarily beneficial to society and synonymous with progress—and regulation as chilling this progress—these narratives pervade the tech industry (and, increasingly, government functioning as well).

### Strategic priorities

Where do we go from here? Across the chapters of this report, we offer a set of approaches that, in concert, will collectively enable us to confront the concentrated power of Big Tech. Some of these are bold policy reforms that offer bright-line rules and structural changes. Others aren't in the traditional domain of policy at all, but acknowledge the importance of non regulatory interventions such as collective action, worker organizing, while acknowledging the role public policy can play in bolstering or kneecapping these efforts. We also identify trendy policy responses that seem positive on their surface, but because they fail to meaningfully address power discrepancies should be abandoned. The primary jurisdictional focus for these recommendations is the US, although where relevant we point to policy windows or trends in other jurisdictions (such as the EU) with necessarily global impacts.

**Four strategic priorities emerge as particularly crucial for this moment:**

---

### 1. Employ strategies that place the burden on companies to demonstrate that they are not doing harm, rather than on the public and regulators to continually investigate, identify, and find solutions for harms after they occur.

Investigative journalism and independent research has been critical to tech accountability: the hard work of those testing opaque systems has surfaced failures that have been crucial for establishing evidence for tech-enabled harms. But, as we outline in the section on Algorithmic Accountability, as a policy response, audits and similar accountability frameworks dependent on third-party evaluation play directly into the tech company playbook by positioning responsibility for identifying and addressing harms outside of the company.

The finance sector offers a useful corollary for thinking this through. Much like AI, the actions taken by large financial firms have diffuse and unpredictable effects on the broader financial system and the economy at large. It's hard to predict any particular harm these may cause, but we know the consequences can be severe, and the communities hit hardest are those that already experience significant inequality. After multiple crisis cycles, there's now widespread consensus that the onus needs to be on *companies* to demonstrate that they are mitigating harms and to comply with regulations, rather than on the broader public to root these out.

The tech sector, likewise has diffuse and unpredictable effects not only on our economy, but our information environment and labor market, among many other things. We see value in a due-diligence approach that requires firms to demonstrate their compliance with the law rather than turn to regulators or civil society to show where they haven't complied—similar in orientation to how we already regulate many goods that have significant public impact, like food and medicine. And we need structural curbs like bright lines and no-go zones that identify types of use and domains of implementation that should be barred in any instance, as many cities have already established by passing bans on facial recognition. For example, in the chapter on Algorithmic Management we identify emotion recognition as a type of technology that should never be deployed, but particularly in the workplace: aside from the clear concerns about its use of pseudoscience and accompanying discriminatory effects, it is fundamentally unethical for employers to seek to draw inferences about their employees' inner state to maximize their profit. And in Biometric Surveillance, we identify the absence of such bright-line measures as the animating force behind a slow creep of facial recognition and other surveillance systems into domains like cars and virtual reality.

We also need to lean further toward scrutiny of harms before they happen rather than waiting to rectify harms after they've already occurred. We discuss what this might look like in the context of merger reviews in the Toxic Competition section, advocating for an approach to merger reviews that looks to predict and prevent abusive practices before they manifest, and in Antitrust, we break down how needed legal reforms would render certain kinds of mergers invalid in the first place, and put the onus on companies to demonstrate they aren't anti-competitive.

### 2. Break down silos across policy areas, so we're better prepared to address where advancement of one policy agenda impacts others. Firms play this isolation to their advantage.

One of the primary sources of Big Tech power is the expansiveness of their reach across markets, with digital ecosystems that stretch across vast swathes of the economy. This means that effective tech policy must be similarly expansive, attending to how measures adopted in the advancement of one policy agenda ramify across other policy domains. For example, as we underscore in the section on Toxic Competition, legitimate concerns about third-party data collection must be addressed in a way that doesn't inadvertently enable further concentration of power in the hands of Big Tech firms. Disconnection between the legal and policy approaches to privacy on the one hand and competition on the other have enabled firms to put forward self-regulatory measures like Google's Privacy Sandbox in the name of privacy that ultimately will lead to the depletion of both privacy and competition by strengthening Google's ability to collect information on consumers directly while hollowing out its competitors. These disconnects can also prevent progress in one policy domain from carrying over to another. Despite years of carefully accumulated evidence on the fallibility of AI-based content filtration tools, we're seeing variants of the magical thinking that AI tools will be able to scan effectively for illegal content, crop up once again in encryption policy with the EU's recent "chat control" client-side scanning proposals.[18]

Policy and advocacy silos can also blunt strategic creativity in ways that foreclose alliance or cross-pollination. We've made progress on this front in other domains, ensuring for example that privacy and national security are increasingly seen as consonant, rather than mutually exclusive, objectives. But AI policy has been undermined too often by a failure to understand AI materially, as a composite of  data, algorithmic models, and large-scale computational power. Once we view AI this way, we can understand data minimization and other approaches that limit data collection not only as protecting consumer privacy, but as mechanisms that help mitigate some of the most egregious AI applications, by reducing firms' data advantage as a key source of their power and rendering certain types of systems impossible to build. It was through data protection law that Italy's privacy regulator was the first to issue a ban on ChatGPT[19] and, the week before that, Amsterdam's Court of Appeal ruled automated firing and opaque algorithmic wages to be illegal.[20] FTC officials also recently called for leveraging antitrust as a tool to enhance worker power, including to push back against worker surveillance.[21] This opens up space for advocates working on AI-related issues to form strategic coalitions with those that have been leveraging these policy tools in other domains.  This multivariate approach has the added advantage of necessitating that those focused on AI-related issues form strategic coalitions with those that have been leveraging these policy tools in other domains.

Throughout this report, we attempt to establish links between related, but often siloed domains: data protection or competition reform as AI policy (see section on Data Minimization); Antitrust]), or AI policy as industrial policy (see section on Algorithmic Accountability).

### 3. Identify when policy approaches get co-opted and hollowed out by industry, and pivot our strategies accordingly.

The tech industry, with its billions of dollars and deep political networks, has been both nimble and creative in its response to anything perceived as a policy threat. There are relevant lessons from the European experience around the perils of shifting from a "rights-based" regulatory framework, as in the GDPR, to a "risk-based" approach, as in the upcoming AI Act and how the framing of "risk" (as opposed to rights)  could tip the playing field in favor of industry-led voluntary frameworks and technical standards.[22]

Responding to the growing chorus calling for bans on facial recognition technologies in sensitive social domains, several tech companies pivoted from resisting regulation to claiming to support it, something they often highlighted in their marketing. The fine print showed that what these companies actually

[18] Ross Anderson, "Chat Control or Child Protection?", *University of Cambridge Computer Lab*, October 13, 2022.
[19] Clothilde Goujard, "Italian Privacy Regulator Bans ChatGPT" *Politico*, March 31, 2023.
[20] Worker Info Exchange, "Historic Digital Rights Win for WIE and the ADCU Over Uber and Ola at the Amsterdam Court of Appeals", April 4, 2023
[21] Elizabeth Wilkins, "Rethinking Antitrust", March 30, 2023
[22] Fanny Hidvegi and Daniel Leufer, "The EU should regulate AI on the basis of rights, not risks", Access Now, February 17, 2021.

supported were soft moves positioned to undercut bolder reform. For example, Washington state's widely critiqued facial recognition law passed with Microsoft's support. The bill prescribed audits and stakeholder engagement, a significantly weaker stance than banning police use which is what many advocates were calling for (see section on Biometrics).

For example, mountains of research and advocacy demonstrate the discriminatory impacts of AI systems and the fact that these issues cannot be addressed solely at the level of code and data. While the AI industry has accepted that bias and discrimination is an issue, companies have also been quick to narrowly cast bias as a technical problem with a technical fix.

Civil society responses must be nimble in responding to Big Tech subterfuge, and we must learn to recognize such subterfuge early. We draw from these lessons when we argue that there is disproportionate policy energy being directed toward AI and algorithmic audits, impact assessments, and "access to data" mandates. Indeed, such approaches have the potential to eclipse and nullify structural approaches to curbing the harms of AI systems  (see section on Algorithmic Accountability). In an ideal world, such transparency-oriented measures would live alongside clear standards of accountability and bright-line prohibitions. But this is not what we see happening. Instead, a steady stream of proposals position algorithmic auditing as the *primary* policy approach toward AI.

Finally, we also need to stay on top of companies' moves to evade regulatory scrutiny entirely: for example, firms have been seeking to introduce measures in global trade agreements (see section on Global Digital Trade) that would render regulatory efforts seeking accountability by signatory countries presumptively illegal. And companies have sought to use promises of AI magic as a means of evading stronger regulatory measures, such as by clinging to the familiar false argument that AI can provide a fix for unsolvable problems, such as in content moderation.[23]

## 4. Move beyond a narrow focus on legislative and policy levers and embrace a broad-based theory of change.

To make progress and ensure the longevity of our wins, we must be prepared for the long game, and author strategies that keep momentum going in the face of inevitable political stalemates. We can learn from ongoing organizing in other domains, from climate advocacy (see section on Climate) that identifies the long-term nature of these stakes, to worker-led organizing (see section on Algorithmic Management) which has emerged as one of the most effective approaches to challenging and changing tech company practice and policy. We can also learn from shareholder advocacy (see section on Tech & Financial Capital), which uses companies' own capital strategies to push for accountability measures - one example is the work of the Sisters of St. Joseph of Peace using shareholder proposals to hold Microsoft to account for human rights abuses. The Sisters also used such proposals to seek a ban on the sale of facial recognition to government entities, and to require Microsoft to evaluate how the company's lobbying aligns with its stated principles.[24] Across these fronts, there is much to learn from the work of organizers and advocates well-versed in confronting corporate power.

[23] Federal Trade Commission, "Combatting Online Harms Through Innovation", Federal Trade Commission, June 2022.
[24] See Chris Mills Rodrigo, "Exclusive: Scrutiny Mounts on Microsoft's Surveillance Technology," *The Hill*, June 17, 2021; and Issie Lapowsky, "These Nuns Could Force Microsoft to Put Its Money Where Its Mouth Is," *Protocol*, November 19, 2021,

### Windows for policy movement

These strategic priorities are designed to take advantage of current windows for action. We summarize them below, and review each in more detail in the body of the report.

| WINDOWS FOR ACTION: THE AI POLICY LANDSCAPE | |
|---|---|
| **Contain tech firms' data advantage.**<br>See: Toxic Competition<br>Data minimization | Data policy *is* AI policy, and steps taken to curb companies' data advantage are a key lever in limiting concentration. |
| | Create bright-line rules that limit firms' ability to collect data on consumers or produce data about them (also known as data minimization). |
| | Connect privacy and competition law both in enforcement and in the development of AI policy. Firms are using these disjuncts to their own advantage. |
| | Reform the merger guidelines and enforcement measures such that consolidation of data advantages receives scrutiny as part of determining whether to allow a merger, and enable enforcers to intervene to stop abusive practices before the harms take place. |
| **Build support for competition reforms as a key lever to reduce concentration in tech.**<br>See: Antitrust | Enforce competition laws by aggressively curbing mergers that expand firms' data advantage and investigating and penalizing companies when they engage in anti-competitive behaviors. |
| | Be wary of US versus China "AI race" rhetoric used for deregulatory arguments in policy debates on competition, privacy, and algorithmic accountability. |
| | Pass the full package of antitrust bills from the 117th Congress to give antitrust enforcers stronger tools to challenge abusive practices specific to the tech industry. |
| | Integrate competition analysis across all tech policy domains – identifying places where platform companies might take advantage of privacy measures to consolidate their own advantage, for example, or how concentration in the cloud market has follow-on effects for security by distributing risk systemically.[25] |
| **Regulate ChatGPT and other large-scale models.**<br>See: General Purpose AI | Apply lessons from the ongoing debate on the EU AI Act to prevent regulatory carveouts for "general-purpose AI": large language models (LLMs) and other similar technologies carry systemic risks; their ability to be fine-tuned toward a range of uses requires more regulatory scrutiny, not less. |

[25] For example, a 2017 outage in Amazon Web Service's S3 server took out several healthcare and hospital systems: Casey Newton, "How a typo took down S3, the backbone of the internet", *The Verge,* March 2, 2017,

| | |
|---|---|
| **Regulate ChatGPT and other large-scale models. (CONT.)** | Mandate documentation requirements that can provide the evidence to ensure developers of these models are held accountable for data and design choices. |
| | Enforce existing law on the books to create public accountability in the rollout of generative AI systems and prevent harm to consumers and competition. |
| | Closely scrutinize claims to ‘openness’; generative AI has structural dependencies on resources available to only a few firms. |
| **Displace audits as the primary policy response to harmful AI.**<br>See: Algorithmic Accountability | Audits and data-access proposals should not be the primary policy response to harmful AI. These approaches fail to confront the power imbalances between Big Tech and the public, and risk further entrenching power in the tech industry. |
| | Closely scrutinize claims from a burgeoning audit economy with companies offering audits-as-a-service despite no clarity on the standards and methodologies for algorithmic auditing, nor consensus on their definitions of risk and harm. |
| | Impose strong structural curbs on harmful AI, such as bans, moratoria, and rules that put the burden on companies to demonstrate that they are fit for public and/or commercial release. |
| **Future-proof against the quiet expansion of biometric surveillance into new domains like cars.**<br>See: Biometrics | Develop comprehensive bright-line rules to future-proof biometric regulation from changing forms and use cases. |
| | Make sure biometric regulation addresses broader inferences, beyond just identification. |
| | Impose stricter enforcement of data minimization provisions that exist in data protection laws globally as a way to curb the expansion of biometric data collection in new domains like virtual reality and automobiles. |
| **Enact strong curbs on worker surveillance.**<br>See: Algorithmic Management | Worker surveillance is fundamentally about employers gaining and maintaining control over workers. Enact policy measures that even the playing field. |
| | Establish baseline worker protections from algorithmic management and workplace surveillance. |
| | Shift the burden of proof to developers and employers and away from workers. |
| | Establish clear red lines around domains (e.g., automated hiring and firing) |

| | |
|---|---|
| | and types of technology (e.g., emotion recognition) that are inappropriate for use in any context. |
| **Prevent "international preemption" by digital trade agreements that can be used to weaken national regulation on algorithmic accountability and competition policy.**<br>See: Digital Trade | Nondiscrimination prohibitions in trade agreements should not be used to protect US Big Tech companies from competition regulation abroad. |
| | Expansive and absolute-secrecy guarantees for source code and algorithms in trade agreements should not be used to undercut efforts to enact laws on algorithmic transparency. |
| | Upcoming trade agreements like the Indo-Pacific Economic Framework should instead be used to set a more a progressive baseline for digital policy. |

It's time to move: years of critical work and organizing has outlined a clear diagnosis of the problems we face, regulators are primed for action, and we have strategies ready to be deployed immediately for this effort. We'll also need more: those engaged in this work are out-resourced and out-flanked amidst a significant uptick in industry lobbying and a growing attack on critical work, from companies firing AI Ethics teams to universities shutting down critical research centers. And we face a hostile narrative landscape. The surge in AI hype that opened 2023 has moved things backwards, re-introducing the notion that AI is associated with 'innovation' and 'progress' and drawing considerable energy toward far-off hypotheticals and away from the task at hand.

We intend this report to provide strategic guidance to inform the work ahead of us, taking a bird's eye view of the landscape and of the many levers we can use to shape the future trajectory of AI - and the tech industry behind it - to ensure that it is the public, not industry, that this technology serves – if we let it serve at all.

Large Scale AI Models

# chatGPT And More: Large Scale AI Models Entrench Big Tech Power

Industry is attempting to stave off regulation, but large-scale AI needs more scrutiny, not less.

1. **Large-scale general purpose AI models (such as GPT-3.5 and its user-facing application chatGPT) are being promoted by industry as "foundational" and a major turning point for scientific advancement in the field. They are also often associated with slippery definitions of "open source."**

   **These narratives distract from what we call the "pathologies of scale" that become more entrenched every day: large-scale AI models are still largely controlled by Big Tech firms because of the enormous computing and data resources they require, and also present well-documented concerns around discrimination, privacy and security vulnerabilities, and negative environmental impacts.**

Large-scale AI models like Large Language Models (LLMs) have received the most hype, and fear-mongering, over the past year. Both the excitement and anxiety[26] around these systems serve to reinforce the notion that these models are 'foundational' and a major turning point for advancement in the field, despite manifold examples where these systems fail to provide meaningful responses to

[26] Future of Life Institute. "Pause Giant AI Experiments: An Open Letter." Accessed March 29, 2023. https://futureoflife.org/open-letter/pause-giant-ai-experiments/.; Harari, Yuval, Tristan Harris, and Aza Raskin. "Opinion | You Can Have the Blue Pill or the Red Pill, and We're Out of Blue Pills." *The New York Times*, March 24, 2023, sec. Opinion. https://www.nytimes.com/2023/03/24/opinion/yuval-harari-ai-chatgpt.html.

prompts.[27] But the narratives associated with these systems distract from what we call the 'pathologies of scale' that this emergent framing serves to both highlight and distract from. The term "foundational," for example, was introduced by Stanford University when announcing a new center of the same name in early 2022,[28] in the wake of the publication of an article listing the many existential harms associated with LLMs.[29] In notably fortuitous timing, the introduction of these models as "foundational'' aimed to equate them (and those espousing them) with unquestionable scientific advancement, a stepping stone on the path to "Artificial General Intelligence"[30] (another fuzzy term evoking science-fiction notions of replacing or superseding human intelligence) thereby making their wide-scale adoption inevitable.[31] These discourses have since returned to the foreground following the launch of Open AI's newest LLM-based chatbot, chatGPT.

On the other hand, the term "general purpose AI" (GPAI) is being used in policy instruments like the EU's AI Act to underscore that these models have no defined downstream use and can be fine-tuned to apply in specific contexts.[32] It has been wielded to make arguments such as because these systems lack clear intention or defined objectives, they should be regulated differently or not at all - effectively creating a major loophole in the law (more on this in Section 2 below).[33]

Such terms deliberately obscure another fundamental feature of these models: they currently require computational and data resources at a scale that ultimately only the most well-resourced companies

[27] See Greg Noone, "'Foundation models' may be the future of AI. They're also deeply flawed," *Tech Monitor*, November 11, 2021 (updated February 9, 2023), https://techmonitor.ai/technology/ai-and-automation/foundation-models-may-be-future-of-ai-theyre-also-deeply-flawed; Dan McQuillan, "We Come to Bury ChatGPT, Not to Praise It," danmcquillan.org, February 6, 2023, https://www.danmcquillan.org/chatgpt.html; Ido Vock, "ChatGPT Proves That AI Still Has a Racism Problem," *New Statesman*, December 9, 2022, https://www.newstatesman.com/quickfire/2022/12/chatgpt-shows-ai-racism-problem; Janice Gassam Asare, "The Dark Side of ChatGPT," *Forbes*, January 28, 2023, https://www.forbes.com/sites/janicegassam/2023/01/28/the-dark-side-of-chatgpt; and Billy Perrigo, "Exclusive: OpenAI Used Kenyan Workers on Less Than $2 Per Hour to Make ChatGPT Less Toxic," *Time*, January 18, 2023, https://time.com/6247678/openai-chatgpt-kenya-workers.

[28] See the Center for Research on Foundation Models, Stanford University, https://crfm.stanford.edu; and Margaret Mitchell (@mmitchell_ai), "Reminder to everyone starting to publish in ML: 'Foundation models' is *not* a recognized ML term; was coined by Stanford alongside announcing their center named for it; continues to be pushed by Sford as *the* term for what we've all generally (reasonably) called 'base models'," Twitter, June 8, 2022, 4:01 p.m., https://twitter.com/mmitchell_ai/status/1534626770820792320.

[29] Emily Bender, Timnit Gebru, Angelina McMillan-Major, Shmargaret Shmitchell, "On the Dangers of Stochastic Parrots: Can Language Models Be Too Big?" FAccT '21: Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency, March 2021, https://dl.acm.org/doi/10.1145/3442188.3445922.

[30] See Sam Altman, "Planning for AGI and beyond", March 2023, https://openai.com/blog/planning-for-agi-and-beyond.

[31] See National Artificial Intelligence Research Resource Task Force, "Strengthening and Democratizing the U.S. Artificial Intelligence Innovation Ecosystem: An Implementation Plan for a National Artificial Intelligence Research Resource," January 2023, https://www.ai.gov/wp-content/uploads/2023/01/NAIRR-TF-Final-Report-2023.pdf; and Special Competitive Studies Project, "Mid-Decade Challenges to National Competitiveness," September 2022, https://www.scsp.ai/wp-content/uploads/2022/09/SCSP-Mid-Decade-Challenges-to-National-Competitiveness.pdf.

[32] The EU Council's draft or "general position" on the AI Act text defines General Purpose AI (GPAI) as an AI system that "that – irrespective of how it is placed on the market or put into service, including as open source software – is intended by the provider to perform generally applicable functions such as image and speech recognition, audio and video generation, pattern detection, question answering, translation and others; a general purpose AI system may be used in a plurality of contexts and be integrated in a plurality of other AI systems." See Council of the European Union, "Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts – General Approach," November 25, 2022, https://data.consilium.europa.eu/doc/document/ST-14954-2022-INIT/en/pdf; see also Future of Life Institute and University College London's proposal to define GPAI as an AI system "that can accomplish or be adapted to accomplish a range of distinct tasks, including some for which it was not intentionally and specifically trained." Carlos I. Gutierrez, Anthony Aguirre, Risto Uuk, Claire C. Boine, and Matija Franklin, "A Proposal for a Definition of General Purpose Artificial Intelligence Systems," Future of Life Institute, November 2022, https://futureoflife.org/wp-content/uploads/2022/11/SSRN-id4238951-1.pdf.

[33] Alex C. Engler, "To Regulate General Purpose AI, Make the Model Move," Tech Policy Press, November 10, 2022, https://techpolicy.press/to-regulate-general-purpose-ai-make-the-model-move.

can afford to sustain.[34] For a sense of the figures, some estimates suggest it will cost 3 million dollars a month to run chatGPT[35] and 20 million dollars in computing costs to train Pathways Language Model (PaLM), a recent LLM from Google.[36] Currently only a handful of companies with incredibly vast resources are able to build them. That's why the majority of existing large-scale AI models have been almost exclusively developed by Big Tech, especially Google (Google Brain, Deepmind), Meta, and Microsoft (and its investee OpenAI). This includes many off-the-shelf, pretrained AI models that are offered as part of cloud AI services, a market already concentrated in Big Tech players, such as AWS (Amazon), Google Cloud (Alphabet), and Azure (Microsoft). Even if costs are lower or come down as these systems are deployed at scale (and this is a hotly contested claim[37]), Big Tech is likely to retain a first mover advantage, having had the time and market experience needed to hone their underlying language models and to develop invaluable in-house expertise. Smaller businesses or start ups may consequently struggle to successfully enter this field, leaving the immense processing power of LLMs concentrated in the hands of a few Big Tech firms.[38]

This market reality cuts through growing narratives that highlight the *potential* for "open-source" and "community or small and medium enterprise (SME)-driven" GPAI projects or even the conflation of GPAI as synonymous with open source (as we've seen in discussions around the EU's AI Act).[39] In September 2022, for example, a group of ten industry associations led by the Software Alliance (or BSA) published a statement opposing the inclusion of any legal liability for the developers of GPAI models.[40] Their headline argument was that this would "severely impact open source development in Europe" as well as "undermine AI uptake, innovation, and digital transformation."[41] The statement leans on hypothetical examples that present a caricature of both how GPAI models work and what regulatory intervention would entail—the classic case cited is of an individual developer creating an open source document-reading tool and being saddled by regulatory requirements around future use cases it can neither predict nor control.

[34] See Ben Cottier, "Trends in the dollar training cost of machine learning systems", *Epoch*, January 31, 2023, https://epochai.org/blog/trends-in-the-dollar-training-cost-of-machine-learning-systems; Jeffrey Dastin and Stephen Nellis, "For tech giants, AI like Bing and Bard poses billion-dollar search problem", *Reuters*, February 22, 2023, https://www.reuters.com/technology/tech-giants-ai-like-bing-bard-poses-billion-dollar-search-problem-2023-02-22/; Jonathan Vanian and Kif Leswing, "ChatGPT and generative AI are booming, but the costs can be extraordinary", *CNBC*, March 13, 2023, https://www.cnbc.com/2023/03/13/chatgpt-and-generative-ai-are-booming-but-at-a-very-expensive-price.html?utm_term=Autofeed&utm_medium=Social&utm_content=Main&utm_source=Twitter#Echobox=1678712441; Dan Gallagher, "Microsoft and Google Will Both Have to Bear AI's Costs", *WSJ*, January 18, 2023, https://www.wsj.com/articles/microsoft-and-google-will-both-have-to-bear-ais-costs-11674006102; Christopher Mims, "The AI Boom That Could Make Google and Microsoft Even More Powerful," *Wall Street Journal*, February 11, 2023, https://www.wsj.com/articles/the-ai-boom-that-could-make-google-and-microsoft-even-more-powerful-9c5dd2a6; and Diane Coyle, "Preempting a Generative AI Monopoly," *Project Syndicate*, February 2, 2023, https://www.project-syndicate.org/commentary/preventing-tech-giants-from-monopolizing-artificial-intelligence-chatbots-by-diane-coyle-2023-02.

[35] See Tom Goldstein (@tomgoldsteincs), "I estimate the cost of running ChatGPT is $100K per day, or $3M per month. This is a back-of-the-envelope calculation. I assume nodes are always in use with a batch size of 1. In reality they probably batch during high volume, but have GPUs sitting fallow during low volume," Twitter, December 6, 2022, 1:34 p.m., https://twitter.com/tomgoldsteincs/status/1600196995389366274; and MetaNews, "Does ChatGPT Really Cost $3M a Day to Run?" December 21, 2022, https://metanews.com/does-chatgpt-really-cost-3m-a-day-to-run.

[36] Lennart Heim, "Estimating 🌴PaLM's training cost," April 5, 2022, https://blog.heim.xyz/palm-training-cost; Peter J. Denning and Ted G. Lewis, "Exponential Laws of Computing Growth," *Communications of the ACM* 60, no. 1 (January 2017):54–65, https://cacm.acm.org/magazines/2017/1/211094-exponential-laws-of-computing-growth/abstract.

[37] Andrew Lohn and Micah Musser, "AI and Compute", *Center for Security and Emerging Technology, https://cset.georgetown.edu/wp-content/uploads/AI-and-Compute-How-Much-Longer-Can-Computing-Power-Drive-Artificial-Intelligence-Progress_v2.pdf*

[38] Richard Waters, "Falling costs of AI may leave its power in hands of a small group", *Financial Times*, March 9, 2023, https://www.ft.com/content/4fef2245-5559-4661-950d-6eb803fea329?accessToken=zwAAAYbcxVeYkc9P7yJFVVlGYd0VDW64A_6jKQ.MEUCIGlMqMyMjHTpGNJ0wUPHEfszGlyW0kEj4nsjoDxiv6kAAiEAlq0Lnl5WWEh8Yc9lLndBenSTWlzX4rs1T45XI03LEgs&sharetype=gift&token=e4fcef47-71f7-4e8d-8958-b51acc82d2b8.

[39] Ryan Morrison, "EU AI Act Should 'Exclude General Purpose Artificial Intelligence' – Industry Groups," *Tech Monitor*, September 27, 2022, https://techmonitor.ai/technology/ai-and-automation/eu-ai-act-general-purpose.

[40] See BSA | The Software Alliance, "BSA Leads Joint Industry Statement on the EU Artificial Intelligence Act and High-Risk Obligations for General Purpose AI," press release, September 27, 2022, ; and BSA, "Joint Industry Statement on the EU Artificial Intelligence Act and High-Risk Obligations for General Purpose AI," September 27, 2022, https://www.bsa.org/files/policy-filings/09272022industrygpai.pdf.

[41] BSA, "BSA Leads Joint Industry Statement on the EU Artificial Intelligence Act and High-Risk Obligations for General Purpose AI."

The discursive move here is to conflate “open source,” which has a specific meaning related to permissions and licensing regimes, with the intuitive notion of being “open” in that they are accessible for downstream use and adaptation (typically through Application Programming Interfaces, or APIs). The latter is more akin to “open access,” though even in that sense they remain limited since they only share the API, rather than the model or training data sources.[42] In fact, in OpenAI’s paper announcing its GPT-4 model, the company said it would not provide details about the architecture, model size, hardware, training compute, data construction or training method used to develop GPT-4, other than noting it used its Reinforcement Learning from Human Feedback approach, asserting competitive and safety concerns. Running directly against the current push to increase firms’ documentation processes,[43] such moves compound what has already been described as a reproducibility crisis in machine learning-based science, in which claims about the capabilities of AI-based models cannot be validated or replicated by others.[44]

Ultimately, this form of deployment only serves to increase Big Tech firms’ revenues and entrench their strategic business advantage.[45] While there are legitimate reasons to consider potential downstream harms associated with making such systems widely accessible,[46] even when projects might make their code publicly available and meet other definitions of open source, the vast computational requirements of these systems mean that dependencies between these projects and the commercial marketplace will likely persist.[47]

[42] Peter Suber, *Open Access* (Cambridge, MA: MIT Press, 2019), https://openaccesseks.mitpress.mit.edu.

[43] Margaret Mitchell, Simone Wu, Andrew Zaldivar, Parker Barnes, Lucy Vasserman, Ben Hutchinson, Elena Spitzer, Inioluwa Deborah Raji, Timnit Gebru, “Model Cards for Model Reporting, *arXiv, January 14, 2019, https://arxiv.org/abs/1810.03993; Emily Bender and Batya Friedman, “Data Statements for Natural Language Model Processing: Toward Mitigating System Bias and Enabling Better Science”, Transactions of the Association for Computational Linguistics,* 6 (2018): 587-604. https://aclanthology.org/Q18-1041/; Timnit Gebru, Jamie Morgenstern, Briana Vecchione, Jennifer Wortman Vaughan, Hanna Wallach, Hal Daumé Iii, and Kate Crawford, "Datasheets for Datasets." *Communications of the ACM* 64, no. 12 (2021): 86-92. https://arxiv.org/abs/1803.09010

[44] Sayash Kapoor and Arvind Narayanan. “Leakage and the Reproducibility Crisis in ML-based Science.” arXiv, July 14, 2022. https://arxiv.org/abs/2207.07048

[45] A report by the UK’s Competition & Markets Authority (CMA) points to how Google’s “open” approach with its Android OS and Play Store (in contrast to Apple’s) proved to be a strategic advantage that eventually led to similar outcomes in terms of revenues and strengthening its consolidation over various parts of the mobile phone ecosystem. See Competition & Markets Authority, “Mobile Ecosystems: Market Study Final Report,” June 10, 2022, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1096277/Mobile_ecosystems_final_report_-_full_draft_-_FINAL__.pdf.

[46] Arvind Narayanan and Sayash Kapoor, “The LLaMA is Out of the Bag. Should We Expect a Tidal Wave of DIsinformation?” *Knight First Amendment Institute (blog),* March 6, 2023. https://knightcolumbia.org/blog/the-llama-is-out-of-the-bag-should-we-expect-a-tidal-wave-of-disinformation

[47] See Coyle, “Preempting a Generative AI Monopoly.”

## On the Dangers of Stochastic Parrots: Can Language Models Be Too Big? By Dr. Emily M. Bender, Dr. Timnit Gebru, Angelina McMillan-Major, and Dr. Margaret Mitchell

> *"Are ever larger LMs inevitable or necessary? What costs are associated with this research direction and what should we consider before pursuing it?"*

In 2021, Dr. Emily M. Bender, Dr. Timnit Gebru, Angelina McMillan-Major, and Dr. Margaret Mitchell warned against the potential costs and harms of large language models (LLMs) in a paper titled *On the Dangers of Stochastic Parrots: Can Language Models Be Too Big?*.[48] The paper led to Google forcing out both Gebru and Mitchell from their positions as the co-leads of Google's Ethical AI team.[49]

**This paper could not have been more prescient in identifying pathologies of scale that afflict LLMs.** As public discourse is consumed by breathless hype around chatGPT and other LLMs as an unarguable advancement in science, this research offers sobering reminders of the serious concerns that afflict these kinds of models. Rather than uncritically accept these technologies as synonymous with progress, the arguments advanced in the paper raise existential questions to *if*, not how, society should be building them at all. The key concerns raised in the paper are as follows:

### Environmental and Financial Costs

LLMs are hugely energy intensive to train and produce large $CO^2$ emissions. Well-documented environmental racism means that marginalized people and people from the Majority World/Global South are more likely to experience the harms caused by heightened energy consumption and $CO^2$ emissions even though they are also least likely to experience the benefits of these models. Additionally, the high cost of entry and training these models means that only a small global elite is able to develop and benefit from LLMs. They argue that environmental and financial costs should become a top consideration in Natural Language Processing (NLP) research.

### Unaccountable Training Data

> *"In accepting large amounts of web text as 'representative' of 'all' of humanity we risk perpetuating dominant viewpoints, increasing power imbalances, and further reifying inequality."*

The use of large and uncurated training data sets risks creating LLMs that entrench dominant, hegemonic views. The large size of these training data sets does not guarantee diversity, as they

[48] Bender, Emily M., Timnit Gebru, Angelina McMillan-Major, and Shmargaret Shmitchell. "On the Dangers of Stochastic Parrots: Can Language Models Be Too Big? 🦜." In *Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency*, 610–23. FAccT '21. New York, NY, USA: Association for Computing Machinery, 2021. https://doi.org/10.1145/3442188.3445922.

[49] Metz, Cade, and Daisuke Wakabayashi. "Google Researcher Says She Was Fired Over Paper Highlighting Bias in A.I." *The New York Times*, December 3, 2020, sec. Technology. https://www.nytimes.com/2020/12/03/technology/google-researcher-timnit-gebru.html.

are often scraped from websites that exclude the voices of marginalized people due to issues such as inadequate Internet access, underrepresentation, filtering practices, or harassment. These data sets run the risk of 'value-lock' or encoding harmful bias into LLMs that are difficult to thoroughly audit.

### Creating Stochastic Parrots

Bender et al. further warn that the pursuit of LLM benchmarks may be a misleading direction for research, as these models have access to form, but not meaning. They observe that "an LM is a system for haphazardly stitching together sequences of linguistic forms it has observed in its vast training data, according to probabilistic information about how they combine, but without any reference to meaning: a stochastic parrot". As stochastic parrots, these models are likely to absorb hegemonic worldviews from their training data and produce outputs that contain both subtle forms of stereotyping and outright abusive language. They can also lead to harms based on translation errors, and through their misuse by bad actors to create propaganda, spread misinformation, and deduce sensitive information.

2. **Large scale AI models must be subject to urgent regulatory scrutiny, particularly given the frenzied speed of rollout to the public. Documentation and scrutiny of data and related design choices at the stage of model development is key to surfacing and mitigating harm.**

   **It's not a blank slate. Legislative proposals on Algorithmic Accountability must be expanded and strengthened and existing legal tools should be creatively applied to introduce friction and shape the direction of innovation.**

   **There is  growing exceptionalism around generative AI models that underplays inherent risks and justifies their exclusion from the purview of AI regulation. We should draw lessons from the ongoing debate in Europe on the inclusion of General Purpose AI under the "high risk" category of the upcoming AI Act.**

Along with breathless hype around the future potential of AI, the release of chatGPT (and its subsequent adaptation into Microsoft's search chatbot) immediately surfaced thorny legal questions, such as, who owns and has rights over the content generated by these systems?[50] Is generative AI protected from lawsuits relating to illegal content they might generate under intermediary liability protections like Section 230?[51]

What's clear is that there are already existing legal regimes that apply to large language models, and we aren't building them from the ground up. In fact, rhetoric that implies this is necessary works mostly to industry's best interests, by slowing the paths to enforcement and updates to the law.

[50] James Vincent, "The scary truth about AI copyright is that nobody knows what will happen next", *The Verge*, November 15, 2022, https://www.theverge.com/23444685/generative-ai-copyright-infringement-legal-fair-use-training-data
[51] Electronic Frontier Foundation, "Section 230", *Electronic Frontier Foundation*, n.d., https://www.eff.org/issues/cda230.

A blog post recently published by the FTC outlined several ways the Agency's authorities already apply to generative AI systems: if they're used for fraud, cause substantial injury, or make false claims about the system's capabilities the FTC has cause to step in. There are many other domains where other legal regimes are likely to apply: intellectual property law, anti-discrimination provisions, and cybersecurity regulations are among them.

There's also a forward looking question of what norms and responsibilities *should apply* to these systems. The growing consensus around recognized harms from AI systems (particularly inaccuracies, bias, and discrimination) has led to a flurry of policy movement over the last few years centering around greater transparency and diligence around data and algorithmic design practices (See also: Algorithmic Accountability). These emerging AI policy approaches will need to be strengthened to address the particular challenges these models bring up, and the current public attention on AI is poised to galvanize momentum where it's been lacking.

In the EU, this question is not theoretical. It is at the heart of a hotly contested debate about whether the original developers of so-called "general purpose AI" (GPAI) models should be subject to the regulatory requirements of the upcoming AI Act.[52] Introduced by the European Commission in April 2021, the Commission's original proposal (Article 52a) effectively exempted the developers of GPAI from complying with the range of documentation and other accountability requirements in the law.[53] This would therefore mean that GPAI that ostensibly had no predetermined use or context would not qualify as 'high risk' – another provision (Article 28) confirmed this position, implying stating that developers of GPAI would only become responsible for compliance if they significantly modified or adapted the AI system for high-risk use. The European Council's position took a different stance where original providers of GPAI will be subject to certain requirements in the law, although working out the specifics of what these would be delegated to the Commission. Recent reports suggest that the European Parliament, too, is considering obligations specific to original GPAI providers.

As the inter-institutional negotiation in the EU has flip-flopped on this issue the debate seems to have devolved into an unhelpful binary where *either* end users *or* original developers take on liability,[54] rather than both having responsibilities of different kinds at different stages.[55] And a recently leaked unofficial US government position paper reportedly states that placing burdens on original developers of GPAI could be "very burdensome, technically difficult and in some cases impossible."[56]

[52] Creative Commons, "As European Council Adopts AI Act Position, Questions Remain on GPAI", *Creative Commons*, December 13, 2022, https://creativecommons.org/2022/12/13/as-european-council-adopts-ai-act-position-questions-remain-on-gpai/; Corporate Europe Observatory, "The Lobbying Ghost in the Machine: Big Tech's covert defanging of Europe's AI Act", February 2023, ' https://corporateeurope.org/sites/default/files/2023-02/The%20Lobbying%20Ghost%20in%20the%20Machine.pdf; Gian Volpicelli, 'ChatGPT broke the EU plan to regulate AI', *Politico*, March 3, https://www.politico.eu/article/eu-plan-regulate-chatgpt-openai-artificial-intelligence-act/

[53] European Commission, "Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts," April 21, 2021, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52021PC0206.

[54] An article by Brookings Fellow Alex Engler, for example, argues that regulating downstream end users makes more sense because "good algorithmic design for a GPAI model doesn't guarantee safety and fairness in its many potential uses, and it cannot address whether any particular downstream application should be developed in the first place." See Alex Engler, "To Regulate General Purpose AI, Make the Model Move", Tech Policy Press, November 10, 2022, https://techpolicy.press/to-regulate-general-purpose-ai-make-the-model-move/; See also Alex Engler, "The EU's attempt to regulate general purpose AI is counterproductive", Brookings, August 24, 2022, https://www.brookings.edu/blog/techtank/2022/08/24/the-eus-attempt-to-regulate-open-source-ai-is-counterproductive/

[55] The Mozilla Foundation's position paper on GPAI helpfully argues in favor of joint liability. See Maximilian Gahntz and Claire Pershan, "Artificial Intelligence Act: How the EU Can Take on the Challenge Posed by General-Purpose AI Systems," *Mozilla Foundation*, 2022, https://assets.mofoprod.net/network/documents/AI-Act_Mozilla-GPAI-Brief_Kx1ktuk.pdf.

[56] Luca Bertuzzi, "The US Unofficial Position on Upcoming EU Artificial Intelligence Rules," Euractiv, October 24, 2022, https://www.euractiv.com/section/digital/news/the-us-unofficial-position-on-upcoming-eu-artificial-intelligence-rules.

These accounts lose sight of the two most important reasons that large-scale AI models require oversight:

1. Data and design decisions made at the developer stage determine many of the model's most harmful downstream impacts, including the risks of bias and discrimination.[57] There is mounting research and advocacy that argues for the benefits of rigorous documentation and accountability requirements on the developers of large-scale models.[58]

2. The developers of these models, many of which are Big Tech or Big Tech-funded, commercially benefit from these models through licensing deals with downstream actors.[59] Companies licensing these models for specific uses should certainly be accountable for conducting diligence within the specific context in which these models are applied, but to make them wholly liable for risks that emanate from data and design choices made at the stage of original development would result in both unfair and ineffective regulatory outcomes.

[57] Sasha Costanza-Chock, Design Justice: Community-Led Practices to Build the Worlds We Need. Cambridge: MIT Press.

[58] See Timnit Gebru, Jamie Morgenstern, Briana Vecchione, Jennifer Wortman Vaughan, Hanna Wallach, Hal Daumé III, and Kate Crawford, "Datasheets for Datasets," arXiv:1803.09010, December 2021, ; Mehtab Khan and Alex Hanna, "The Subjects and Stages of AI Dataset Development: A Framework for Dataset Accountability," *Ohio State Technology Law Journal*, forthcoming, accessed March 3, 2023, ; and Bender, Gebru, McMillan-Major, and Shmitchell, "On the Dangers of Stochastic Parrots."

[59] See for example Madhumita Murgia, "Big Tech companies use cloud computing arms to pursue alliances with AI groups", *Financial Times*, February 5, 2023, https://www.ft.com/content/5b17d011-8e0b-4ba1-bdca-4fbfdba10363?shareType=nongift; Leah Nylen and Dina Bass, "Microsoft Threatens Data Restrictions In Rival AI Search", *Bloomberg*, March 25, 2023, https://www.bloomberg.com/news/articles/2023-03-25/microsoft-threatens-to-restrict-bing-data-from-rival-ai-search-tools; OpenAI, Pricing, https://openai.com/api/pricing; Jonathan Vanian, "Microsoft adds OpenAI technology to Word and Excel", CNBC, March 16, 2023, https://www.cnbc.com/2023/03/16/microsoft-to-improve-office-365-with-chatgpt-like-generative-ai-tech-.html; and Patrick Seitz, "Microsoft Stock Breaks Out After Software Giant Adds AI To Office Apps", Investor's Business Daily, March 17, 2023, https://www.investors.com/news/technology/microsoft-stock-fueled-by-artificial-intelligence-in-office-apps/.

Toxic Competition

# Regulating Big Tech’s Data Advantage

One of the key sources of tech firms' power is their data advantage. Privacy and competition law are two tools that, used in concert, can effectively curb this source of some of tech firms' most harmful behavior. Doing so requires strategic calibration of the effects of each on digital markets and on the broader public, implementing a policy approach that takes in to account the benefits firms seek to take advantage of via information asymmetries.

In this section we identify two domains in which these dynamics are currently playing out: data mergers and adtech. These provide an illustrative example for analysis of the tech industry playbook and a path forward.

**Privacy and competition law are too often siloed from one another, leading to interventions that easily compromise the objectives of one issue over the other. Firms are taking advantage of this to amass information asymmetries that contribute to further concentration of their power. Rather than accept the silos of legal expertise and precedent, it's clear that privacy and competition regulators need to work in concert to regulate an industry that draws on invasive surveillance for competitive benefit.[60]**

Considered in isolation, traditional antitrust and privacy analyses could indeed lead in divergent directions. But, as Maurice Stucke and Ariel Ezrachi underscore in their work, competition can be toxic.[61] As Stucke puts it, "in the digital platform economy, behavioral advertising can skew the platforms', apps, and websites' incentives. The ensuing competition is about us, not for us. Here firms compete to exploit us in discovering better ways to addict us, degrade our privacy, manipulate our behavior, and capture the surplus."[62] Scholars in the EU have taken this line of thinking as far as to explore how competition law could be enforced as a substitute for data protection law given the endemic nature of such practices within digital markets.[63] And though privacy measures that aim to curb data collection are in some instances a significant step toward curbing tech firms' data advantage, they only go so far —for example, some proposals that focus on third-party tracking in isolation offer a giant loophole that enables tech firms to entrench their power.[64]

Bringing privacy and competition policy into closer consideration can, at best, offer a complementary set of levers for tech accountability that work in concert with one another to check the power of big tech firms.[65] If left unattended, pursuing privacy and competition in isolation will enable corporate actors to "resolve" critiques through self-regulatory moves that ultimately expand and entrench, rather than limit, concentrated tech power.[66]

We see this playing out in two domains in particular: data mergers and adtech.

[60] Jacques Crémer, Yves-Alexandre de Montjoye and Heike Schweitzer, "Competition policy for the digital era", European Commission, 2019, https://ec.europa.eu/competition/publications/reports/kd0419345enn.pdf; Autorité de la concurrence and Bundeskartellamt, "Competition Law and Data", *Bundeskartellamt*, May 10, 2016, https://www.bundeskartellamt.de/SharedDocs/Publikation/DE/Berichte/Big%20Data%20Papier.pdf?__blob=publicationFile&v=2; Competition & Markets Authority and the Information Commissioner's Office, "Competition and Data Protection in Digital Markets: A Joint Statement between the CMA and the ICO," May 19, 2021, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/987358/Joint_CMA_ICO_Public_statement_-_final_V2_180521.pdf; Subcommittee on Antitrust, Commercial, and Administrative Law of the Committee on the Judiciary of the House of Representatives, "Investigation of Competition in Digital Markets," July 2022, https://www.govinfo.gov/content/pkg/CPRT-117HPRT47832/pdf/CPRT-117HPRT47832.pdf; Australian Competition & Consumer Commission, "Digital Platforms Inquiry: Final Report and Executive Summary," video, July 26, 2019, https://www.accc.gov.au/focus-areas/inquiries-finalised/digital-platforms-inquiry-0/final-report-executive-summary; and the Competition Commission, "Online Intermediation Platforms Market Inquiry: Provisional Summary Report," July 2022, https://www.compcom.co.za/wp-content/uploads/2022/07/OIPMI-Provisional-Summary-Report.pdf.

[61] Maurice E. Stucke and Ariel Ezrachi, *Competition Overdose: How Free Market Mythology Transformed Us from Citizen Kings to Market Servants* (New York: HarperCollins, 2020)

[62] Maurice E. Stucke, "The Relationship between Privacy and Antitrust," *Notre Dame Law Review Reflection* 97, no. 5 (2022): 400–417, https://ndlawreview.org/wp-content/uploads/2022/07/Stucke_97-Notre-Dame-L.-Rev.-Reflection-400-C.pdf

[63] Giuseppe Colangelo and Mariateresa Maggiolino "Data Protection in Attention Markets: Protecting Privacy Through Competition?", *Journal of European Competition Law & Practice*, April 3, 2017, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2945085

[64] Maurice E. Stucke, "The Relationship between Privacy and Antitrust," *Notre Dame Law Review Reflection* 97, no. 5 (2022): 400–417, https://ndlawreview.org/wp-content/uploads/2022/07/Stucke_97-Notre-Dame-L.-Rev.-Reflection-400-C.pdf

[65] Peter Swire, "Protecting Consumers: Privacy Matters in Antitrust Analysis," Center for American Progress, October 19, 2007, https://www.americanprogress.org/article/protecting-consumers-privacy-matters-in-antitrust-analysis.

[66] See Cudos, "The Fable of Self-Regulation: Big Tech and the End of Transparency," n.d., https://www.cudos.org/blog/the-fable-of-self-regulation-big-tech-and-the-end-of-transparency-%F0%9F%8C%AB%EF%B8%8F; and Rys Farthing and Dhakshayini Sooriyakumaran, "Why the Era of Big Tech Self-Regulation Must End," *Australian Quarterly* 92 no. 4 (October–December 2021): 3–10, https://www.jstor.org/stable/27060078.

# Data Mergers and Acquisitions

### Competition analysis must account for how firms leverage commercial surveillance tools and strategies to amass power

Competition enforcers have largely now converged in agreement that data plays a critical role in digital markets and that regulators need to attend to how data practices shape information asymmetries and market power.[67] It then follows that competition analysis must account for how firms leverage commercial surveillance tools and strategies to their competitive advantage and to the detriment of user privacy.[68]

One primary means through which tech firms have grown their market power is through the consolidation of data they are able to collect—and when they can't do so on their own, they buy their way in. Google's acquisition of DoubleClick in 2008 was a bellwether case that led to a practice now widespread in the industry: the acquisition of firms in order to gain an information advantage.[69]

Google-DoubleClick was itself not a conventional data merger. Google acquired DoubleClick because its own publisher ad server had failed to gain traction in the adtech industry.[70] Through DoubleClick, Google gained control of both the market-leading publisher and ad server, and an advertising exchange. And at the time of the acquisition, Google emphasized that its privacy policies prohibited the company from combining its own data streams with those obtained from other websites. But the company quietly walked back this internal policy in 2016 - notably, a point at which the company had amassed greater market power and thus was less exposed to the risk users would flock to a competitor platform.[71] Following the change, Google could combine all its user data into a single user identification that it could integrate into its buying tools to enable uniquely precise targeting of particular users—an extremely valuable advantage for Google Ads' advertising clients.[72] This also made it harder for publishers to track users themselves by masking these user identifiers.[73] These negative effects led publishers to complain that the acquisition was anticompetitive; the FTC, however, opted not to block the merger from going forward.[74]

[67] See Federal Trade Commission, "Remarks of Chair Lina M. Khan as Prepared for Delivery," IAPP Global Privacy Summit 2022, Washington, D.C., April 11, 2022, https://www.ftc.gov/system/files/ftc_gov/pdf/Remarks%20of%20Chair%20Lina%20M.%20Khan%20at%20IAPP%20Global%20Privacy%20Summit%202022.pdf; ; Jacques Crémer, Yves-Alexandre de Montjoye and Heike Schweitzer, "Competition policy for the digital era", European Commission, 2019, https://ec.europa.eu/competition/publications/reports/kd0419345enn.pdf; Autorité de la concurrence and Bundeskartellamt, "Competition Law and Data", *Bundeskartellamt*, May 10, 2016, https://www.bundeskartellamt.de/SharedDocs/Publikation/DE/Berichte/Big%20Data%20Papier.pdf?__blob=publicationFile&v=2; The United States Department of Justice, "Assistant Attorney General Jonathan Kanter of the Antitrust Division Delivers Remarks at the Keystone Conference on Antitrust, Regulation & the Political Economy", The United States Department of Justice, March 2, 2023, https://www.justice.gov/opa/speech/assistant-attorney-general-jonathan-kanter-antitrust-division-delivers-remarks-keystone; Federal Trade Commission, "FTC Hearing #6: Privacy, Big Data, and Competition", FTC, November 6-8, 2018, https://www.ftc.gov/news-events/events/2018/11/ftc-hearing-6-privacy-big-data-competition

[68] Katharine Kemp, "Concealed data practices and competition law: why privacy matters", *European Competition Journal* 16, no. 2-3 (2020): 628-672, https://doi.org/10.1080/17441056.2020.1839228

[69] See Louise Story and Miguel Helft, "Google Buys DoubleClick for $3.1 Billion," *New York Times*, April 14, 2007, https://www.nytimes.com/2007/04/14/technology/14DoubleClick.html; and Steve Lohr, "This Deal Helped Turn Google into an Ad Powerhouse. Is That a Problem?" *New York Times*, September 21, 2020, https://www.nytimes.com/2020/09/21/technology/google-doubleclick-antitrust-ads.html.

[70] Tony Yiu, "Why Did Google Buy DoubleClick?" *Towards Data Science*, Medium, May 5, 2020, https://towardsdatascience.com/why-did-google-buy-doubleclick-22e706e1fb07.

[71] Justin Wise, "Val Demings repeatedly presses Google's Pichai on 'staggering' consolidation of consumer data", *The Hill*, July 29, 2020, https://thehill.com/policy/technology/509642-val-demings-repeatedly-presses-googles-pichai-on-consolidation-of-consumer/.

[72] See United States et al. v. Google LLC, Case 1:23-cv-00108 (United States District Court for the Eastern District or Virginia, Alexandria Division, January 24, 2023), https://storage.courtlistener.com/recap/gov.uscourts.vaed.533508/gov.uscourts.vaed.533508.1.0_1.pdf.

[73] *United States et al. v. Google LLC* at 39.

[74] Federal Trade Commission, "Statement of Federal Trade Commission Concerning Google/DoubleClick", FTC File No. 071-0170, December 20, 2007, https://www.ftc.gov/system/files/documents/public_statements/418081/071220googledc-commstmt.pdf.

## List of data mergers

| Date | Companies | Amount | Completed? |
|---|---|---|---|
| 2007 | Google — DoubleClick | $3.1b | Yes |
| 2013 | Facebook — Onavo | $120m | Yes |
| 2014 | Facebook — WhatsApp | $19b | Yes |
| 2016 | Microsoft — LinkedIn | $26.2b | Yes |
| 2018 | Apple — Shazam | $400M | Yes |
| 2019 | Google — Fitbit | $2.1b | Yes |
| 2020 | Facebook — Giphy | $315m | No - CMA forced to sell |
| 2022 | Alphabet — BrightBytes | Unknown | Yes |
| 2022 | Amazon — OneMedical | $3.9b | Yes |
| 2022 | Amazon — iRobot | $1.7b | No - EU set to launch an antitrust case |

More explicit instances of data mergers followed, including instances where companies used nonpublic data obtained through an acquisition in order to shape their decisionmaking. In another notable example, Facebook's acquisition of the virtual private network (VPN) Onavo enabled the company to gain competitive insights by monitoring users' network traffic: internal documents released by UK regulators demonstrate that Facebook was closely tracking the market reach of Facebook's competitors by drawing on Onavo traffic data.[75] Facebook then paid users between the ages of 13 and 35 up to $20 per month to sign up for a rebranded version of Onavo called "Facebook Research" to enable the company to gather even more granular data on their usage habits. Apple eventually blocked the app for breaking Apple's policies,[76] but the data Facebook collected from Onavo played a significant role in Facebook's decision to acquire WhatsApp, in one of the most famous cases of a larger firm buying and neutralizing a fast-growing competitor, thereby further extending its reach and collection of data.[77]

## Competition Law Requires Understanding How Data Impacts Market Behavior

Given the clear anti-competitive effects of such mergers, the question that follows is why they were allowed to proceed. Traditional merger analysis offers some foothold for making such claims: the legal analysis involved in competition cases usually involves some form of harm identification to evaluate whether a merger deserves closer scrutiny or is likely to substantially lessen competition or create a monopoly. Given the nature of digital markets, data can take shape as an element of a company's market power - and as Elettra Bietti argues, this may best be framed in terms of a firm's ability to produce and capture data through its control over infrastructure.[78] This makes understanding companies' data collection practices relevant to competition law: understanding how firms use commercial surveillance to monitor users, competitors, and the market at large is crucial to account for how these firms build their competitive advantage.[79]

Merger enforcement is increasingly taking such an analysis into account, but the shift has been incremental. For example, while then relatively novel, testimony submitted to the FTC at the time of the proposed DoubleClick acquisition argued that the Commission should consider potential harms under two standard elements of a merger analysis: by examining how the privacy harms enabled by the acquisition could *reduce consumer welfare* and lead to a *reduction in the quality of a good or service*—both elements that would fit easily into the FTC's framework for examining the merger.[80] The FTC opted not to take up these considerations, and allowed the acquisition to move forward with few

[75] See Karissa Bell, "'Highly Confidential' Documents Reveal Facebook Used VPN App to Track Competitors," Mashable, December 5, 2018, https://mashable.com/article/facebook-used-onavo-vpn-data-to-watch-snapchat-and-whatsapp; and UK Parliament, "Note by Damian Collins MP, Chair of the DCMS Committee," December 5, 2018, https://www.parliament.uk/globalassets/documents/commons-committees/culture-media-and-sport/Note-by-Chair-and-selected-documents-ordered-from-Six4Three.pdf.

[76] Josh Constine, "Apple Bans Facebook's Research App That Paid Users for Data," TechCrunch, January 30, 2019, https://techcrunch.com/2019/01/30/apple-bans-facebook-vpn.

[77] Ariel Ezrachi and Maurice E. Stucke, *Virtual Competition: The Promise and Perils of the Algorithm-Driven Economy* (Cambridge, MA: Harvard University Press, 2019), 43.

[78] Elettra Bietti, "Data, Context and Competition Policy", Promarket, March 31, 2023.

[79] Lina M. Khan, "Sources of Tech Platform Power," *Georgetown Law Technology Review* 2, no. 2 (2018): 325–334, https://georgetownlawtechreview.org/sources-of-tech-platform-power/GLTR-07-2018.; Howard A. Shelanski, "Information, Innovation, and Competition Policy for the Internet", *University of Pennsylvania Law Review*, Vol. 161 (2013), 1663-2013, https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=1025&context=penn_law_review provides an earlier perspective that nevertheless concludes that competition policy must account for nonprice effects and consider the cost of underenforcement of competition laws in digital markets.

[80] Peter Swire, "Protecting Consumers: Privacy Matters in Antitrust Analysis," Center for American Progress, October 19, 2007, https://www.americanprogress.org/article/protecting-consumers-privacy-matters-in-antitrust-analysis.

restrictions, and in a similar decision the European Commission affirmed it saw a clear separation between the applicability of EU antitrust laws and data protection rules for evaluating the merger.[81]

More recently, a 2019 market study by the UK's Competition and Markets Authority (CMA) on online platforms and digital advertising concluded that the lack of controls over the collection and use of personal data by big tech firms indicates that these firms do not face strong enough competitive constraints.[82] And regulators are already integrating an analysis that accounts for the role of data into their competition cases. For example, in 2021, when the CMA rejected Meta's attempt to acquire Giphy, it acknowledged that the merger would enable Meta to increase its market power by changing the terms of access, such as requiring that Giphy customers like TikTok, Twitter, and Snapchat give up more data from UK users in order to access Giphy GIFs.[83] And in a concurring statement issued alongside the Federal Trade Commission's decision not to block a merger between Amazon and One Medical, Commissioners Rebecca Kelly Slaughter and Alvaro Bedoya cautioned that Amazon now has access to potentially private health information, because US privacy rules on health related data (HIPPA) exempt 'de-identified' data writ large that can nevertheless be used by the company to its own advantage. The statement underscores that the lack of a purpose limitation in HIPPA "cuts against longstanding American information policy".[84]

## Merger Guideline Updates Could Be A Boost for Effective Enforcement

One of the hindering factors in a more muscular enforcement of merger law to curb data practices is a lack of resources for enforcement agencies, as the frequency of such mergers increases exponentially. This has led regulators in both the US and EU to seek more powerful tools to enable them to more effectively tackle the challenge of data mergers, specifically by seeking tools that would enable them to intervene at earlier stages before harms to competition have occurred.

For example, the FTC and Justice Department are currently considering modernizations to the merger guidelines that may similarly allow antitrust enforcers to intervene before harms to competition are affected (known as the 'incipiency standard'),[85] and to further enable them to more effectively handle digital markets, zero-price ("free") products, multi sided markets, and data aggregation.[86] The Platform Competition and Opportunity Act, part of the package of antitrust bills currently before the US Congress, would declare acquisitions of direct and potential future competitors presumptively invalid, shifting the burden of proof to dominant platforms to demonstrate why a merger would not be

[81] Giuseppe Colangelo and Mariateresa Maggiolino "Data Protection in Attention Markets: Protecting Privacy Through Competition?", *Journal of European Competition Law & Practice*, April 3, 2017, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2945085

[82] Competition and Markets Authority, "Online Platforms and Digital Advertising Market Study," July 3, 2019, https://www.gov.uk/cma-cases/online-platforms-and-digital-advertising-market-study.

[83] Competition and Markets Authority, "CMA Orders Meta to Sell Giphy," October 18, 2022, https://www.gov.uk/government/news/cma-orders-meta-to-sell-giphy.

[84] Federal Trade Commission, "Statement of Commissioner Alvaro M. Bedoya Joined by Commissioner Rebecca Kelly Slaughter Regarding Amazon.com, Inc.'s Acquisition of 1Life Healthcare, Inc.", *FTC*, February 27, 2023, https://www.ftc.gov/system/files/ftc_gov/pdf/2210191amazononemedicalambstmt.pdf

[85] Andrew I. Gavil, "Competitive Edge: The silver lining for antitrust enforcement in the Supreme Court's embrace of "textualism"" Equitable Growth, July 28, 2021, https://equitablegrowth.org/competitive-edge-the-silver-lining-for-antitrust-enforcement-in-the-supreme-courts-embrace-of-textualism/; Baker, Jonathan ; Farrell, Joseph; Gavil, Andrew; Gaynor, Martin; Kades, Michael; Katz, Michael; Kimmelman, Gene; Melamed, A.; Rose, Nancy; Salop, Steven; Scott Morton, Fiona; and Shapiro, Carl, "Joint Response to the House Judiciary Committee on the State of Antitrust Law and Implications for Protecting Competition in Digital Markets" *Congressional and Other Testimony*, 18, 2020, https://digitalcommons.wcl.american.edu/pub_disc_cong/18/

[86] Federal Trade Commission, "Federal Trade Commission and Justice Department Seek to Strengthen Enforcement Against Illegal Mergers," January 18, 2022, https://www.ftc.gov/news-events/news/press-releases/2022/01/federal-trade-commission-justice-department-seek-strengthen-enforcement-against-illegal-mergers.

anticompetitive.[87] And the European Commission (EC) amended its merger referral guidelines to create a lower burden of proof for authorities to justify tests of merger deals for lack of competitiveness in digital markets, enabling them to intervene earlier on by encouraging national competition authorities to refer mergers to the EC when at least one of the companies concerned does not reflect its future competitive potential.[88]

## ADTECH

**Bright-line rules restricting first-party data collection for advertising purposes will effectively tackle toxic competition.**

> "The shift from third- to first-party data collection is being propelled by both regulatory momentum and proactive Big Tech initiatives. Ostensibly privacy-enhancing, this shift only entrenches Big Tech's data advantage, with deleterious effects on both privacy and competition."

Critiques of business models that rely on surveillance and profiling of consumers have reached a crescendo in recent years.[89] While some bolder advocacy proposals suggest a complete ban on behavioral targeting business models,[90] or require divestment of ownership across multiple parts of the

[87] Platform Competition and Opportunity Act of 2021, H.R. 3826, 117th Congress (2021–2022), https://www.congress.gov/bill/117th-congress/house-bill/3826/text.

[88] European Commission, "Communication from the Commission: Commission Guidance on the Application of the Referral Mechanism Set Out in Article 22 of the Merger Regulation to Certain Categories of Cases, *Official Journal of the European Union* 113 (2021): 1–6. A proposal by the UK government in discussions around the DMA would have gone even further to reverse the burden of proof in digital mergers for dominant firms, though it was ultimately not adopted, see Christopher T. Marsden and Ian Brown, "App stores, antitrust and their links to net neutrality: A review of the European policy and academic debate leading to the EU Digital Markets Act." Internet Policy Review, Vol 12, no. 1 (2023), https://doi.org/10.14763/2023.1.1676

[89] See Federal Trade Commission, "Remarks of Chair Lina M. Khan as Prepared for Delivery," IAPP Global Privacy Summit 2022, Washington, D.C., April 11, 2022, https://www.ftc.gov/system/files/ftc_gov/pdf/Remarks%20of%20Chair%20Lina%20M.%20Khan%20at%20IAPP%20Global%20Privacy%20Summit%202022.pdf; ; Carissa Véliz, "Privacy Is Power: Why and How You Should Take Back Control of Your Data," *International Data Privacy Law* 12, no. 3 (August 2022): 255–257, https://doi.org/10.1093/idpl/ipac007; Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (New York: Public Affairs, 2020); Kylie Jarrett, Feminism, Labour and Digital Media: The Digital Housewife (London: Routledge, Taylor et Francis Group, 2017); Lina Dencik and Javier Sanchez-Monedero, "Data Justice," *Internet Policy Review* 11, no. 1 (January 14, 2022), https://doi.org/10.14763/2022.1.1615; Safiya Umoja Noble, *Algorithms of Oppression: How Search Engines Reinforce Racism* (New York: NYU Press, 2018); ); Haleluya Hadero, "As Amazon Grows, So Does Its Surveillance of Consumers," Chicago Tribune, August 23, 2022, https://www.chicagotribune.com/business/ct-biz-amazon-surveillance-ap-20220823-illdnv2jejeqlh6l56z2jo3dp4-story.html; Chris Gilliard, "The Rise of 'Luxury Surveillance,'" Atlantic, October 18, 2022, https://www.theatlantic.com/technology/archive/2022/10/amazon-tracking-devices-surveillance-state/671772; BBC, "Google Sign-Up 'Fast Track to Surveillance,' Consumer Groups Say,' June 30, 2022, https://www.bbc.co.uk/news/technology-61980233; Natasha Lomas, "Meta's Surveillance Biz Model Targeted in UK 'Right to Object' GDPR Lawsuit," TechCrunch, November 21, 2022, https://techcrunch.com/2022/11/21/meta-surveillance-gdpr-right-to-object-lawsuit; and Katherine Tangalakis-Lippert, "Amazon's Empire of Surveillance: Through Recent Billion-Dollar Acquisitions of Health Care Services and Smart Home Devices, the Tech Giant Is Leveraging Its Monopoly Power to Track 'Every Aspect' of Our Lives," *Business Insider*, August 28, 2022, https://www.businessinsider.com/amazon-empire-of-surveillance-leveraging-monopoly-power-tracking-purchases-2022-8.

[90] Congresswoman Anna G. Eshoo, "Eshoo, Schakowsky, Booker Introduce Bill to Ban Surveillance Advertising," press release, January 18, 2022, https://eshoo.house.gov/media/press-releases/eshoo-schakowsky-booker-introduce-bill-ban-surveillance-advertising.

digital advertising ecosystem[91], a large majority of regulatory regimes[92] and legislative proposals[93] have instead homed in on restricting the collection of third-party data through cookie tracking.

Big Tech firms have swiftly responded to these headwinds by supporting, and even leading, this transition away from third-party tracking toward first-party collection of users' data.[94] In lieu of longstanding methods of third-party data collection, large firms are exploiting the fact that they directly control the vast majority of the environment in which data is collected: they are able to take advantage of the network effects associated with the scale at which they operate by collecting, analyzing, and using data within platforms they wholly own and control.[95] This is a product of an environment in which these firms are so dominant that it is virtually impossible not to use their systems.[96]

Companies like Google might best be characterized as ecosystems:[97] "the providers of the very infrastructure of the internet, so embedded in the architecture of the digital world that even their competitors [have] to rely on their services," as journalist Kashmir Hill put it.[98] Maintaining an ecosystem enables dominant firms to derive insights from multiple points in a market, and to leverage them across their lines of business. Concerns that this harms competition have led competition enforcers to conclude that some intervention may be needed to level the playing field in arenas such as mobile apps[99] and cloud computing.[100]

Given this state of affairs, Big Tech firms no longer need third-party tracking—in fact, shifting to first-party tracking only helps reinforce their dominant position, building a moat that can stave off any potential incipient competitors. Policy stances that focus primarily on third-party tracking are already out of date in light of this situation. Without more aggressive approaches to curbing first-party data collection and its anticompetitive effects, we could find ourselves in a world where concentration of power in the tech industry is greatly increased, rather than limited, by efforts at privacy accountability.

[91] Senator Mike Lee, "Lee Introduces Digital Advertising Act," press release, May 19, 2022.
[92] State of California Department of Justice, Rob Bonta, Attorney General, "California Consumer Privacy Act (CCPA)," February 15, 2023, https://oag.ca.gov/privacy/ccpa; General Data Protection Regulation, https://gdpr-info.eu/.
[93] See American Data Privacy and Protection Act, H.R. 8152, 117th Congress (2021–2022), https://www.congress.gov/bill/117th-congress/house-bill/8152/text; and Banning Surveillance Advertising Act of 2022, H.R. 6416, 117th Congress (2021–2022), https://www.congress.gov/bill/117th-congress/house-bill/6416.
[94] See Brian X. Chen and Daisuke Wakabayashi, "You're Still Being Tracked on the Internet, Just in a Different Way," *New York Times*, April 6, 2022, https://www.nytimes.com/2022/04/06/technology/online-tracking-privacy.html; and Perry Keller, "After Third Party Tracking: Regulating the Harms of Behavioural Advertising Through Consumer Data Protection," May 4, 2022, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4115750, 4.
[95] Michael Veale, "Adtech's New Clothes Might Redefine Privacy More than They Reform Profiling," Netzpolitik.org, February 25, 2022, https://netzpolitik.org/2022/future-of-online-advertising-adtechs-new-clothes-might-redefine-privacy-more-than-they-reform-profiling-cookies-meta-mozilla-apple-google.
[96] See Kashmir Hill, "I Cut the 'Big Five' Tech Giants from My Life. It Was Hell," Gizmodo, February 7, 2019, https://gizmodo.com/i-cut-the-big-five-tech-giants-from-my-life-it-was-hel-1831304194; and Nordine Abidi and Ixart Miquel-Flores, "Too Tech to Fail?" Faculty of Law Blogs, University of Oxford, July 13, 2022, https://blogs.law.ox.ac.uk/business-law-blog/blog/2022/07/too-tech-fail.
[97] Whether or not the largest cloud providers are characterized as ecosystems is the focus of an ongoing study by the UK's Ofcom. See Ofcom, "Cloud Services Market Study," October 6, 2022, https://www.ofcom.org.uk/__data/assets/pdf_file/0025/244825/call-for-inputs-cloud-market-study.pdf.
[98] Kashmir Hill, "I Tried to Live without the Tech Giants. It Was Impossible," *New York Times*, July 31, 2020, https://www.nytimes.com/2020/07/31/technology/blocking-the-tech-giants.html.
[99] See National Telecommunications and Information Administration, United States Department of Commerce, "Competition in the Mobile App Ecosystem," February 1, 2023, https://ntia.gov/report/2023/competition-mobile-app-ecosystem; and Competition and Markets Authority, "Mobile Ecosystems Market Study," June 15, 2021, https://www.gov.uk/cma-cases/mobile-ecosystems-market-study.
[100] See Ofcom, "Cloud Services Market Study", *Ofcom*, 6 October, 2022, https://www.ofcom.org.uk/__data/assets/pdf_file/0025/244825/call-for-inputs-cloud-market-study.pdf; Authority for Consumers & Markets, "Market Study into Cloud Services," September 5, 2022, https://www.acm.nl/en/publications/market-study-cloud-services; Autorité de la concurrence, "The Authorité de la concurrence Starts Proceedings Ex Officio to Analyse Competition Conditions in the Cloud Computing Sector," January 27, 2022, https://www.autoritedelaconcurrence.fr/en/communiques-de-presse/autorite-de-la-concurrence-starts-proceedings-ex-officio-analyse-competition; Japan Fair Trade Commission, "Report Regarding Cloud Services," June 28, 2022, https://www.jftc.go.jp/en/pressreleases/yearly-2022/June/220628.html; and Fair Trade Commission, "KFTC Announces Results of Cloud Service Market Study," December 28, 2022, https://www.ftc.go.kr/solution/skin/doc.html?fn=06ceef699d6065867e4c69b26c1b3be720409a638b2cd9e3c5b91c70324ab5b4&rs=/fileupload/data/result/BBSMSTR_000000002402.

### The Privacy Sandbox Effect

Google's Privacy Sandbox offers a useful case in point. The company has historically relied heavily on the use of third-party cookies for targeted advertising, which has been central to how it makes money.[101] Following the passage of the General Data Protection Regulation (GDPR) and other data protection regulations indicating behavioral advertising would be under the regulatory spotlight, Google began to develop a strategy that would enable the company to reduce its reliance on third-party cookies given increasing regulatory constraints, but nevertheless maintain its control of the market.[102] This culminated in Google's announcement of its Privacy Sandbox initiative:[103] a self-regulatory move aimed at heading off more stringent forms of regulation that could directly target its capacity to draw inferences about and profile consumers.

The announcement soon led to complaints by publishers that the proposed moves would serve to undermine their ability to generate revenue through advertising by limiting their ability to target users, and that this would ultimately entrench Google's market power.[104] This prompted the UK Competition and Markets Authority to open an investigation into these concerns. The CMA informed Google that its proposals would likely amount to an "abuse of dominance position." Under UK law, this describes a situation when one or a group of enterprises uses its dominant position in a market to either directly exploit consumers or exclude other competitors from the market.[105]

Following a traditional competition analysis, the likely outcome would be to require more widespread sharing of the data Google collects with publishers: it would treat data as an essential resource to the market, and the cure would be to ensure that it was more widely available to other market players. But such a remedy would carry widespread harms to consumer privacy—harms that would necessarily exploit consumer interests and lead to a race to the bottom by expanding, rather than limiting, commercial surveillance practices. An integrated analysis would thus institute curbs to these kinds of data collection practices in the first place, ensuring that nobody, regardless of their market position, gets to benefit from the exploitation of consumers' data, whether collected via third-party or first-party tracking.[106]

To avert enforcement action by the CMA, Google offered a set of commitments that it hoped would bring the proposed framework into compliance with UK competition law. Arguably the strongest of these commitments was the implementation of "data silos" to ensure that Google has the same level of access to data that others do—a commitment very much in line with a traditional competition analysis. But even here, it will be challenging for enforcement agencies to ensure that Google is following through on this promise: they've set up an internal monitoring committee that will ostensibly audit the

[101] Sarah Myers West, "Data Capitalism: Redefining the Logics of Surveillance and Privacy," Business & Society 58, no. 1 (January 2019): 20–41, https://doi.org/10.1177/0007650317718185.
[102] David Eliot and David Murakami Wood, "Culling the FLoC: Market Forces, Regulatory Regimes and Google's (Mis)steps on the Path Away from Targeted Advertising," *Information Polity* 27, no. 2 (2022): 259–274, https://dl.acm.org/doi/abs/10.3233/IP-211535.
[103] Google, The Privacy Sandbox, https://privacysandbox.com
[104] Competition and Markets Authority, "CMA to Investigate Google's 'Privacy Sandbox' Browser Changes," press release, January 8, 2021, https://www.gov.uk/government/news/cma-to-investigate-google-s-privacy-sandbox-browser-changes.
[105] Office of Fair Trading, "Abuse of a Dominant Position: Understanding Competition Law," December 2004, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/284422/oft402.pdf.
[106] See for example Maurice E. Stucke, "The Relationship between Privacy and Antitrust," *Notre Dame Law Review Reflection* 97, no. 5 (2022): 400–417, https://ndlawreview.org/wp-content/uploads/2022/07/Stucke_97-Notre-Dame-L.-Rev.-Reflection-400-C.pdf.. Stucke's analysis is consistent with the FTC's recently updated policy statement on its Section 5 Unfair Methods of Competition authorities. See FTC, "Policy Statement Regarding the Scope of Unfair Methods of Competition Under Section 5 of the Federal Trade Commission Act, Commission File No. P221202," November 10, 2022, https://www.ftc.gov/system/files/ftc_gov/pdf/P221202Section5PolicyStatement.pdf.

system for compliance, but this puts the burden on the regulator rather than on Google to avert any harms, and it remains unclear how effective this regime will be or what will happen when/if it fails. Other commitments included offering consultation with third parties about Privacy Sandbox, enabling the CMA to test the effects of its implementation of Privacy Sandbox proposals via a monitoring trustee, and "incorporating user controls" into the system. In exchange for accepting the voluntary commitments, the CMA agreed not to continue its investigation.[107] But in the absence of a more structural separation or bright-line rules, we're essentially left having to either take Google's word for it, or developing expensive and untested inspection tools to evaluate whether they do what they say they will do.

> "Big Tech firms get away with inflicting privacy harms on us because of the absence of competition in tech, making it especially important for antitrust analysis to be integrated broadly across tech policy domains. Breaking down the silos between tech policy issues will enable a clearer picture of the larger whole."

Looking to the realm of cybersecurity may be instructive: security professionals have long expressed concerns about tech monopolies because they create a single target and point of failure that can have significant downstream consequences if breached. A report produced in 2003 by the Computer and Communications Industry Association, a group of leading security experts, warned that Microsoft's employment of software designs that lock users into their products led to a dangerous environment in which the world's dominant operating system was riddled with vulnerabilities, exposing its end users to viruses.[108]

As the researchers noted, "Microsoft must not be allowed to impose new restrictions on its customers—imposed in the way only a monopoly can do—and then claim that such exercise of monopoly power is somehow a solution to the security problems inherent in its products. The prevalence of security flaws in Microsoft's products is an effect of monopoly power; it must not be allowed to become a reinforcer."[109] The report is particularly notable not only given our present-day climate, but also for its depiction of how dominant tech firms are incentivized to present solutions to problems *caused* by monopoly power that *reinforce* their monopoly power. The researchers cautioned that regulators must treat security policy as intertwined with competition policy, not separate from it.

Today, many other policy domains in focus for the tech accountability community are similarly intertwined with competition. In addition to security, privacy, content moderation, and algorithmic

[107] Competition and Markets Authority, "Case 50972 – Privacy Sandbox – Google Commitments Offer," February 4, 2022, https://assets.publishing.service.gov.uk/media/62052c6a8fa8f510a204374a/100222_Appendix_1A_Google_s_final_commitments.pdf.
[108] See Robert Lemos, "Report: Microsoft Dominance Poses Security Risk," September 24, 2003, https://www.cnet.com/news/privacy/report-microsoft-dominance-poses-security-risk; and Danny Penman, "Microsoft Monoculture Allows Virus Spread," September 25, 2003, https://www.newscientist.com/article/dn4203-microsoft-monoculture-allows-virus-spread.
[109] "Cyberinsecurity: The Cost of Monopoly: How the Dominance of Microsoft's Products Poses a Risk to Security," *AUUGN* 24, no. 4 (December 2003): 49.

discrimination— among others— at once shape and are shaped by competition dynamics within digital markets. Yet the effects of concentration in the tech industry are rarely integrated into policy analysis across these domains, and antitrust remains largely separated from other tech policy arenas both in terms of the regulatory regimes and the expertise needed to engage with them. In order to seek accountability more effectively within the tech industry, **these silos must necessarily be broken down to gain a clear picture of the larger whole.**

Regulators are already moving swiftly to ensure that issues relating to privacy and competition work in concert, or at least stay in conversation with one another.[110] But civil society has a long way to go to catch up: we need a more robust advocacy effort that melds these concerns, for example by fighting for restrictions on first-party data collection given its impact on both privacy and competition, or by advocating for merger scrutiny where a firm is attempting to expand its market power through buying its way into a data advantage. It's crucial that policy advocacy acknowledges the interplay between these domains and pushes for measures in which one does not compromise the other.

[110] Examples include the European Data Protection Supervisor's 2014 workshop on Privacy, Consumers, Competition and Big Data, https://edps.europa.eu/data-protection/our-work/publications/reports/report-edps-workshop-privacy-consumers-competition-and_en, the FTC's updated statement on Unfair Methods of Competition, FTC, "Policy Statement Regarding the Scope of Unfair Methods of Competition Under Section 5 of the Federal Trade Commission Act", November 10, 2022, https://www.ftc.gov/legal-library/browse/policy-statement-regarding-scope-unfair-methods-competition-under-section-5-federal-trade-commission; its announcement of revisions to the Merger Guidelines, FTC, "Federal Trade Commission and Justice Department Seek to Strengthen Enforcement Against Illegal Mergers," press release, January 18, 2022, https://www.ftc.gov/news-events/news/press-releases/2022/01/federal-trade-commission-justice-department-seek-strengthen-enforcement-against-illegal-mergers, Competition and Markets Authority, "CMA-ICO Joint Statement on Competition and Data Protection Law," May 19, 2021, https://www.gov.uk/government/publications/cma-ico-joint-statement-on-competition-and-data-protection-law; and Australian Competition & Consumer Commission, "Digital Platform Services Inquiry 2020–25: September 2022 Interim Report," November 11, 2022, https://www.accc.gov.au/focus-areas/inquiries-ongoing/digital-platform-services-inquiry-2020-25/september-2022-interim-report.

Algorithmic Accountability

# Moving beyond audits

Despite unresolved concerns, an audit-centered algorithmic accountability approach is being rapidly mainstreamed into voluntary frameworks and regulations, and industry has taken a leadership role in its development.

Technical modes of evaluation have long been critiqued for narrowly positioning ‘bias’ as a flaw within an algorithmic system that can be fixed and eliminated. While calls from civil society to move towards broader ‘socio-technical’ evaluation expand the frame in needed directions, these have failed to make the leap from theory to practice. Such approaches are prone to vague and underspecified benchmarks, and both technical and socio-technical audits place the primary burden for algorithmic accountability on those with the fewest resources.

Across the board, audits run the risk of entrenching power within the tech industry, and take focus away from more structural responses.

---

**An emerging policy regime composed of a combination of audits, impact assessments, and mandates for access to company data is rapidly being mainstreamed as the primary means of addressing and mitigating the harms caused by AI-powered systems.**

**Far from distancing itself from this policy momentum, the tech industry is strategically assuming a leadership position in the field of AI auditing.**

A growing wave of policy endorses the use of audits for AI systems in both public- and private-sector contexts. In the EU, the Digital Services Act (DSA), which came into force in 2022, includes multiple provisions that require audits[111] and creates more pathways to access company data for regulators as well as vetted researchers.[112] In the US, there are multiple legislative proposals that endorse elements of this approach for regulating the tech industry, including the Algorithmic Accountability Act, which was

[111] See Sections 28 and 31 of the European Union’s Digital Services Act (DSA), October 27, 2022.
[112] See Section 31 of the DSA.

reintroduced in 2022[113] and tasks the FTC with implementing impact assessments for AI-enabled decision-making, or the Platform Accountability and Transparency Act of 2022[114] that creates pathways for external researchers to get access to data. There is also increasing momentum behind voluntary mechanisms like the National Institute of Standards and Technology (NIST)'s recently published 2023 Risk Management Framework, which endorses independent third-party audits,[115] as well as a large and growing research community (including industry-funded and/or affiliated actors)[116] engaged in developing frameworks following this approach.

## First-, Second-, and Third-Party Audits

Researchers have helpfully classified algorithmic audits into first-, second-, or third-party audits as a way to differentiate the entities and incentives at play.[117] First-party, or internal, audits are those conducted by teams within an organization and tasked with reviewing tools created in-house. Several tech companies have specialized teams and tools for this purpose. Second-party audits involve contracted vendors who offer auditing-as-a-service, which includes traditional consulting organizations like PwC and Deloitte, as well as a growing number of independent ventures (both for profit and nonprofit) that specialize in certain kinds of audits ("bias audits") or sectors.[118] Third-party audits stand apart: they have been conducted by journalists, independent researchers, or entities with no contractual relationship to the audit target. From Gender Shades[119] to the audit of London's LFR system[120] to ProPublica's audit of predictive policing tech,[121] these audits have been pivotal in galvanizing advocacy around AI-related harms.[122]

This wave of policy activity has created business opportunities, as evidenced by a fast-developing industry around AI audits.[123] Far from distancing itself from this policy momentum, the industry is strategically assuming a leadership position in the field of AI auditing, creating and even licensing their

[113] Algorithmic Accountability Act of 2022, H.R. 6580, 117th Congress (2021–2022).
[114] Chris Coons, "Senator Coons, Colleagues Introduce Legislation to Provide Public with Transparency of Social Media Platforms," press release, December 21, 2022.
[115] National Institute of Standards and Technology (NIST), US Department of Commerce, "Artificial Intelligence Risk Management Framework (AI RMF 1.0)," January 2023.
[116] See for example Rolls Royce, "The Aletheia Framework™: Helping Build Trust in Artificial Intelligence," n.d., accessed March 3, 2023; PwC, "PwC's Responsible AI: AI You Can Trust," n.d., accessed March 3, 2023; and Deloitte, "Deloitte AI Institute Teams with Chatterbox Labs to Ensure Ethical Application of AI," press release, March 15, 2021.
[117] See Sasha Costanza-Chock, Inioluwa Deborah Raji, and Joy Buolamwini, "Who Audits the Auditors? Recommendations from a Field Scan of the Algorithmic Auditing Ecosystem," *FAccT '22: 2022 ACM Conference on Fairness, Accountability, and Transparency* (June 2022): 1571–1583; and Kate Kaye, "A New Wave of AI Auditing Startups Wants to Prove Responsibility Can Be Profitable," *Protocol*, January 3, 2022.
[118] See Parity (which changed its name to Vera in January 2023), accessed March 3, 2023; Vera, accessed March 3, 2023; https://foundation.mozilla.org/en/blog/its-time-to-develop-the-tools-we-need-to-hold-algorithms-accountable. See also Deborah Raji, "It's Time to Develop the Tools We Need to Hold Algorithms Accountable," Mozilla Foundation, February 2, 2022; and Laurie Clarke, "AI Auditing Is the Next Big Thing. But Will It Ensure Ethical Algorithms?" *Tech Monitor*, April 14, 2021.
[119] Algorithmic Justice League Project, MIT Media Lab, Gender Shades, 2018, accessed March 3, 2023.
[120] Evani Radiya-Dixit, "A Sociotechnical Audit: Assessing Police Use of Facial Recognition," Minderoo Centre for Technology and Democracy, October 2022.
[121] Julia Angwin, Jeff Larson, Surya Mattu, and Lauren Kirchner, "Machine Bias," *ProPublica*, May 23, 2016.
[122] Inioluwa Deborah Raji and Joy Buolamwini, "Actionable Auditing: Investigating the Impact of Publicly Naming Biased Performance Results of Commercial AI Products," *Conference on Artificial Intelligence, Ethics, and Society*, 2019.
[123] See Costanza-Chock, Raji, and Buolamwini, "Who Audits the Auditors?" And Sebastian Klovig Skelton, "AI accountability held back by 'audit-washing' practices," *Computer Weekly*, November 23, 2022.

own auditing tools and mechanisms. Microsoft,[124] Salesforce,[125] Google,[126] Meta,[127] Twitter,[128] IBM,[129] and Amazon[130] all launched widely publicized initiatives around internal technical audit tools, with the purported goal of mitigating harms like bias. (Twitter's ethics and accountability team was infamously dissolved in the aftermath of Elon Musk's takeover, and Microsoft laid off its entire AI ethics and society team in March 2023.)[131] The tech industry has also been vocally supportive of voluntary approaches with little or no enforcement mechanisms, most notably NIST's recent Risk Management Framework guidelines. For example, in a 2022 US House hearing on Trustworthy AI,[132] the vice president of the US Chamber of Commerce, Jordan Crenshaw, speaking on behalf of industry, said: "We believe it's premature to get into prescriptive regulation. We support voluntary frameworks like we see at NIST."

**The process-based nature of these rules allow them to be easily internalized by companies as a cost of doing business. With the encouragement of industry, this "algorithmic accountability" tool kit is displacing structural approaches that would require more fundamental changes.**

Audits, impact assessments, and mandates for access to company data have various features in common:

- They are responses to what is popularly referred to as AI's "black-box problem", i.e., the concern that AI systems have a range of characteristics that make it impossible to identify or diagnose harm from the outside without access to the technical components and logics of the system.
- They focus on verifying performance and other characteristics of the system, but this is typically evaluated at the technical level, rather than within real-life contexts of use and largely to the exclusion of interrogating the business model and related power dynamics.
- They are procedural (rather than substantive) mechanisms. They intervene through process-based modes like requiring inspection, documentation, evaluation, or greater transparency, as opposed to bright-line rules.
- They are generally intended to surface and address harms such as discrimination and bias, consumer manipulation/deception, and data privacy and security-related concerns rather than competition-related concerns. Efforts to enable audits or access to data for competitors or

[124] Microsoft, "Responsible AI Impact Assessment Template," June 2022.
[125] See Salesforce, "Salesforce Debuts AI Ethics Model: How Ethical Practices Further Responsible Artificial Intelligence," September 2, 2021; and Kathy Baxter, "AI Ethics Maturity Model," Salesforce, n.d., accessed March 3.
[126] See Khari Johnson, "Google researchers release audit framework to close AI accountability gap," VentureBeat, January 30, 2020; and Hansa Srinivasan, "ML-Fairness-Gym: A Tool for Exploring Long-Term Impacts of Machine Learning Systems," Google Research (blog), February 5, 2020.
[127] See Issie Lapowsky, "Facebook's Decision on Trump Posts Is a 'Devastating' Setback, Says Internal Audit," *Protocol*, July 8, 2020; Issie Lapowsky, "One Year in, Meta's Civil Rights Team Still Needs a Win," *Protocol*, April 9, 2022; Jerome Pesenti, "Facebook's Five Pillars of Responsible AI," Meta AI, June 22, 2021; and Roy L. Austin, "Following Through on Meta's Civil Rights Audit Progress," Meta, November 18, 2021.
[128] See Anna Kramer, "Twitter's Image Cropping Was Biased, So It Dumped the Algorithm," *Protocol*, May 19, 2021; and Anna Kramer, "How Twitter Hired Tech's Biggest Critics to Build Ethical AI," *Protocol*, June 23, 2021.
[129] AI Fairness 360, IBM / Linux Foundation AI & Data, accessed March 3, 2023.
[130] Jeffrey Dastin and Paresh Dave, "Amazon to Warn Customers on Limitations of Its AI," Reuters, November 30, 2022.
[131] Will Knight, "Elon Musk Has Fired Twitter's 'Ethical AI' Team," *Wired*, November 4, 2022; and Zoë Schiffer and Casey Newton, "Microsoft just laid off one of its responsible AI teams", *Platformer*, March 14, 2023.
[132] *Trustworthy AI: Managing the Risks of Artificial Intelligence, House Event 115165*, 117th Congress (2021–2022), September 29, 2022.

regulators for the purpose of enhancing competition exist[133] but are currently siloed from the algorithmic accountability discourse.

The focus on greater levels of visibility, diligence, and reflexivity in data and computational processes is valuable, especially given the structural opacity that plagues industry AI.[134] The process-based of these algorithmic accountability tools is also relatively less controversial for industry,[135] and therefore more politically feasible, compared to prescriptive rule-based approaches that put bright-line restrictions in place. However, at a time when disproportionate energy appears to be channeled toward this policy template as a core focus of many civil society and government actors,[136] often to the exclusion of other remedies, we must urgently confront its limits.

This is especially true in the context of large, complex, and well-resourced companies that operate with arguably limitless financial and technical resources and growing influence over policy spaces. (See also: Tech & Financial Capital) What do we lose when we make audit-centered algorithmic accountability the focus of our policy strategy for the tech industry? In a scathing critique of the research community's focus on algorithmic fairness and accountability, Sean McDonald and Ben Gansky argued that these approaches can preclude "the ability of stakeholders to ask first principles questions (i.e. even if a system executes its task perfectly, would it be just?) and channels moral energy away from more fundamental reforms."[137]

**There is a burgeoning audit economy with companies offering audits-as-a-service despite no clarity on the standards and methodologies for algorithmic auditing, nor consensus on the definitions of risk and harm.**

**Coherent standards and methodologies for assessing when an algorithmic system is harmful to its users are hard to establish, especially when it comes to complex and sprawling Big Tech platforms. Audit tools will forever be compromised by this conundrum, making it more likely than not that audits will devolve into a superficial "checkbox" exercise.**

This algorithmic accountability regime, and audits in particular, have proliferated as self-regulatory mechanisms within industry without an existing, clear policy framework setting standards for harm. This has resulted in an anomalous situation where there is widespread confusion around fundamental questions: *What are we auditing for? Which harms count and how are they being defined?*

[133] See European Commission, "Antitrust: Commission Accepts Commitments by Amazon Barring It from Using Marketplace Seller Data, and Ensuring Equal Access to Buy Box and Prime," press release, December 20, 2022; Kate Cox, "Amazon's Use of Marketplace Data Breaks Competition Law, EU Charges," *Ars Technica*, November 10, 2020; Natasha Lomas, "Europe Lays Out Antitrust Case against Amazon's Use of Big Data," TechCrunch, November 10, 2020; and Competition and Markets Authority, "Competition and Data Protection in Digital Markets: A Joint Statement between the CMA and the ICO 2021 (CMA, ICO)," March 25, 2022.

[134] For an unpacking of the many layers of opacity in commercial systems, see Jenna Burrell, "How the Machine 'Thinks': Understanding Opacity in Machine Learning Algorithms," *Big Data & Society* 3, no. 1 (January–June 2016).

[135] The vice president of the US Chamber of Commerce also vocally supported the NIST RMF's voluntary approach. See Alex LaCasse, "US NIST publishes AI Risk Management Framework 1.0," International Association of Privacy Professionals (IAPP), January 27, 2023; Deloitte, "Deloitte AI Institute Teams with Chatterbox Labs to Ensure Ethical Application of AI," press release, March 15, 2021; and Rumman Chowdhury, "Sharing Learnings about Our Image Cropping Algorithm," Twitter Engineering (blog), May 19, 2021.

[136] See Ellen P. Goodman and Julia Tréhu, "AI Audit-Washing and Accountability," German Marshall Fund of the United States (GMF), November 2022; Christine Custis, "Operationalizing AI Ethics through Documentation: ABOUT ML in 2021 and Beyond," Partnership on AI (PAI), April 14, 2021; Stanford University Human-Centered Artificial Intelligence, "AI Audit Challenge," 2022, accessed March 2, 2023; and Ada Lovelace Institute and DataKind UK, "Examining the Black Box: Tools for Assessing Algorithmic Systems," April 2020.

[137] Ben Gansky and Sean McDonald, "CounterFAccTual: How FAccT Undermines Its Organizing Principles," *FAccT '22: 2022 ACM Conference on Fairness, Accountability, and Transparency* (June 2022): 1982–1992.

Europe's DSA, the first example of a legal algorithmic auditing requirement for the tech industry, keeps this standard very broad. It requires companies to audit for "systemic risks to fundamental rights," although with special emphasis on harms related to manipulation and illegal content. While this could theoretically allow for expansive evaluation of potential harms, it also leaves enormous discretion for the auditing entity (the company selling the software, or a third party) to limit the scope of the audit to those issues least threatening to their interests. Deloitte, for example, has already proposed applying its own methodologies in the absence of "specific parameters and audit methodology."[138]

At the same time, this lack of specificity could be the symptom of a more foundational challenge with presenting audits as a general accountability measure, rather than a problem in itself. Cathy O'Neil, the founder of one of the first algorithmic auditing firms, herself declared that she would never take on the task of "auditing Facebook" because the scale and granularity of harms was too diffused, systemic, and intractable to lend itself to any simplified template for an audit.[139] When it comes to social media content algorithms, for example, a major focus for algorithmic accountability debates, the question of harm, methodology, and expertise required will in large part be determined by the specificities of the geographical and/or social context in which such harm transpires, and the particular groups that are impacted. This is also where the relative lack of support or initiative from Big Tech for non-Western and other minoritized countries and contexts has become glaring.[140]

These broadly scoped audits can be helpfully contrasted against inspections done by regulators in the context of enforcement challenges, from the Australian Competition regulator's audit of travel website Trivago's algorithms,[141] the investigations into Clearview AI's facial recognition system,[142] or UK privacy regulator ICO's investigation of microtargeting in political campaigns in 2017.[143] These inspections had narrowly defined objectives—that is, to assess whether the company was in violation of a clearly articulated standard of harm—and were typically evaluated alongside a range of other contextual evidence, including testimony from company executives. Similarly, data protection impact assessments under the GDPR have served to create a documentation trail around compliance with the specific provisions of the regulation, which regulators can use for monitoring.

While attention has largely been on technical audits, there might be greater promise from the possibility of accountability mechanisms that more directly surface organizational incentives and business models. A recent report from a consortium of UK-based regulators, while highlighting the lack of standards and methodology around technical auditing, identified "governance audits" as a tool that requires companies to provide detailed documentation on operational structures for design, development, management, and internal mechanisms oversight for algorithmic systems.[144] Given pervasive corporate secrecy in the tech industry around decision-making and human involvement in algorithmic processes, public disclosure of this information could be a more impactful intervention.

[138] See Goodman and Tréhu, "AI Audit-Washing and Accountability."
[139] Cathy O'Neil, "Facebook's Algorithms Are Too Big to Fix," Bloomberg, October 8, 2021.
[140] Conducted in the face of major public backlash, Meta's human rights impact assessment of its role in the Myanmar genocide of 2017, for example, was widely decried as superficial "ethics washing." See Dan Milmo, "Rohingya Sue Facebook for £150bn over Myanmar Genocide," *Guardian*, December 6, 2021.
[141] Peter Leonard, "The Deceptive Algorithm in Court: Australian Competition and Consumer Commission v Trivago N.V. [2020] FCA 16," Society for Computers and Law, January 31, 2020.
[142] Information Commissioner's Office (ICO), "ICO Fines Facial Recognition Database Company Clearview AI Inc More than £7.5m and Orders UK Data to Be Deleted," May 23, 2022.
[143] Information Commissioner's Office (ICO), "Democracy Disrupted? Personal Information and Political Influence," July 11, 2018.
[144] Competition and Markets Authority, "Auditing Algorithms: The Existing Landscape, Role of Regulators and Future Outlook," September 23, 2022.

**The response to the failures of technical audits includes recommendations for more participation from directly impacted communities in the audit process and calls to adapt testing to resemble real-life contexts. However, these proposals remain largely theoretical and are at risk of being superficially incorporated into a "checkbox" exercise. Many of these proposals place the primary burden for algorithmic accountability on those with the fewest resources—researchers, or even on the communities most harmed by these systems.**

The field of "bias testing" is both the most mature in the accountability tool kit compared to other algorithmic harms and the most glaring in its deficiencies. Most industry activity and research on computational audits has focused on quantifying the fairness of algorithmic decisions and proposing technical measures for mitigating bias and discrimination. Several policy proposals in the US specifically include requirements for audits and impact assessments to evaluate for bias against protected groups.[145] Most industry activity and research on computational audits has focused on quantifying the fairness (a contested term, as we'll see below) of algorithmic decisions and proposing technical measures to mitigate these concerns. It's also worth noting that legal antidiscrimination discourse has influenced the ways in which fairness has been conceptualized in technical fields.[146]

Yet the fundamental limits of computational approaches to fairness, carefully demonstrated through journalism, advocacy, and research over the past five years,[147] are more widely acknowledged than ever before. These critiques include:

- Computational approaches to fairness remain limited to evaluating for bias in laboratory-like conditions, abstracted from the real social and political contexts in which these systems are generated and used.[148] This includes the ways in which the system, in practice, plays into existing power asymmetries; and the limitations of any kind of "human review" of these systems, which is typically superficial due to the tendency to defer to algorithmic decisions; and

[145] See Richard Vanderford, "New York's Landmark AI Bias Law Prompts Uncertainty," *Wall Street Journal*, September 21, 2022; and DC Chamber of Commerce, "DC Chamber of Commerce Small Business Action Alert: Stop Discrimination by Algorithms Act Of 2021," n.d., accessed March 3, 2023; https://www.npr.org/local/305/2021/12/10/1062991462/d-c-attorney-general-introduces-bill-to-ban-algorithmic-discrimination. The Algorithmic Justice and Online Platform Transparency Act would prohibit discriminatory use of personal information in algorithmic processes; see Algorithmic Justice and Online Platform Transparency Act, S. 1896, 117th Congress (2021–2022).

[146] See Anna Lauren Hoffman, "Where Fairness Fails: Data, Algorithms, and the Limits of Antidiscrimination Discourse," *Information, Communication & Society* 22, no. 7 (2019): 900–915; and 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," *Hawaii International Conference on System Sciences*, January 2019. See also Samuel R. Bagenstos, "The Structural Turn and the Limits of Antidiscrimination Law," *California Law Review* 94, no. 1 (January 2006): 1–47; and Kimberle Crenshaw, "Demarginalizing the Intersection of Race and Sex: A Black Feminist Critique of Antidiscrimination Doctrine, Feminist Theory and Antiracist Politics," *University of Chicago Legal Forum* 1989, no. 1 (1989).

[147] See Meredith Whittaker, Kate Crawford, Roel Dobbe, Genevieve Fried, Elizabeth Kaziunas, Varoon Mathur, Sarah Myers West, Rashida Richardson, Jason Schultz, and Oscar Schwartz, *AI Now Report 2018*, AI Now Institute, 2018; https://arxiv.org/abs/2101.09869; Abeba Birhane, Elayne Ruane, Thomas Laurent, Matthew S. Brown, Johnathan Flowers, Anthony Ventresque, and Christopher L. Dancy, "The Forgotten Margins of AI Ethics," *FAccT '22: 2022 ACM Conference on Fairness, Accountability, and Transparency*, May 9, 2022; Pratyusha Kalluri, "Don't Ask If Artificial Intelligence Is Good or Fair, Ask How It Shifts Power," *Nature*, July 7, 2020; Os Keyes, "Automating Autism: Disability, Discourse, and Artificial Intelligence," *Journal of Sociotechnical Critique* 1, no. 1 (2020): 1–31; Os Keyes, Jevan Hutson, and Meredith Durbin, "A Mulching Proposal: Analysing and Improving an Algorithmic System for Turning the Elderly into High-Nutrient Slurry," *CHI EA '19: Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems*, May 2019; Cynthia L. Bennett and Os Keyes, "What Is the Point of Fairness? Disability, AI and the Complexity of Justice," August 9, 2019; Sarah Myers West, "Redistribution and Rekognition: A Feminist Critique of Algorithmic Fairness," *Catalyst: Feminism, Theory, Technoscience* 6, no. 2 (2020): 1–24; Andrew D Selbst, Danah Boyd, Sorelle A Friedler, Suresh Venkatasubramanian, and Janet Vertesi, "Fairness and Abstraction in Sociotechnical Systems," *In Proceedings of the Conference on Fairness, Accountability, and Transparency* (2019); and Sofia Kypraiou, "What Is Fairness?" *Feminist AI*, September 13, 2021.

[148] Ben Green and Lily Hu, "The Myth in the Methodology: Towards a Recontextualization of Fairness in Machine Learning," *35th International Conference on Machine Learning*, 2018; Shira Mitchell, Eric Potash, Solon Barocas, Alexander D'Amour, and Kristian Lum, "Algorithmic Fairness: Choices, Assumptions, and Definitions," *Annual Review of Statistics and Its Application* 8 (2021): 141–163; and Rodrigo Ochigame, "The Long History of Algorithmic Fairness," *Phenomenal World*, January 30, 2020.

the added risks that these decisions work to legitimize discriminatory decisions and allow management to evade responsibility.[149]

- There's a need for greater attention to the structural bias embedded in the contexts in which data is collected for training AI systems.[150] This defeats the notion that "more data" or "better data" will mitigate AI challenges.[151]
- The reduction of fairness evaluation to solely quantifiable metrics disguises the inherently subjective and value-laden assumptions built into these systems.[152]
- These approaches, by unquestioningly placing people in particular groups or classes, fail to account for how social and racial group classifications are themselves socially constructed through the "widespread use of racial categories as if they represent natural and objective differences between groups."[153]

Under the Biden Administration, there is certainly greater acknowledgment that problems of bias and discrimination cannot be reduced to technical metrics, and an explicit embrace of 'socio-technical' approaches that have been championed by the algorithmic accountability research community. A 2022 report on AI bias by NIST, the US government's primary technical standard-setting organization, identified "human bias" and "systemic bias," along with technical bias, as key to evaluating the impact of a system in practice.[154] These findings were reflected to some degree in the first version of NIST's Risk Management Framework, released in January 2023, which proposes several robust recommendations, including:

- Evaluating for impacts of AI systems across their life cycle
- Accounting for the sociotechnical context in which the application is being deployed, and using both qualitative and quantitative measures
- Developing approaches for "evaluating systemic and human-cognitive sources of bias"
- Documenting decisions, risk-related trade-offs, and system limitations
- Normalizing the ability to reconfigure or reconsider the product in early stages
- Processes for involving stakeholders in decision-making and examining internal cultural dynamics and norms

[149] See Ben Green and Amba Kak, "The False Comfort of Human Oversight as an Antidote to A.I. Harm," *Slate*, June 15, 2021; and Ben Green, "The Flaws of Policies Requiring Human Oversight of Government Algorithms," *Computer Law & Security Review* 45 (2022).

[150] See Rashida Richardson, Jason Schultz, and Kate Crawford, "Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice," *New York University Law Review* 94 (May 2019): 192–233; Safiya Umoja Noble, *Algorithms of Oppression: How Search Engines Reinforce Racism* (New York: NYU Press, 2018); and Sarah Myers West, Meredith Whittaker, and Kate Crawford, "Discriminating Systems: Gender, Race, and Power in AI," AI Now Institute, April 2019.

[151] See Bennett and Keyes, "What Is the Point of Fairness?"

[152] Lindsay Weinberg, "Rethinking Fairness: An Interdisciplinary Survey of Critiques of Hegemonic ML Fairness Approaches," *Journal of Artificial Intelligence Research* 74 (2022): 75–109.

[153] Alex Hanna, Emily Denton, Andrew Smart, Jamila Smith-Loud, "Towards a Critical Race Methodology in Algorithmic Fairness," *Conference on Fairness, Accountability, and Transparency (FAT* '20)*, January 27–30, 2020; J. Khadijah Abdurahman, "FAT* Be Wilin'," Medium, February 24, 2019; Morgan Klaus Scheuerman, Madeleine Pape, and Alex Hanna, "Auto-Essentialization: Gender in Automated Facial Analysis as Extended Colonial Project," *Big Data & Society* 8, no. 2 (2021); and Michele Elam, "Signs Taken for Wonders: AI, Art & the Matter of Race," *Daedalus* 151, no. 2 (Spring 2022): 198–217.

[154] Reva Schwartz, Apostol Vassilev, Kristen Greene, Lori Perine, Andrew Burt, and Patrick Hall, "Towards a Standard for Identifying and Managing Bias in Artificial Intelligence," National Institute of Standards and Technology (NIST), US Department of Commerce, March 2022.

While this policy is a pivotal shift in how bias evaluation is conceptualized, the distance between this theoretical vision and the practice of algorithmic auditing as it stands today represents a chasm that these proposed reforms cannot bridge. Crucially, NIST's policy document is explicitly voluntary,[155] which begs the question: *Why would developers of AI models feel empowered or incentivized to course-correct or shape products in ways that might contradict the firm's business goals?*[156] If algorithmic bias is—and it often is—inextricably linked to power asymmetries and structural inequity, how can those be effectively surfaced in procedural mechanisms like audits, and to what end? Incorporating the participation of impacted communities has become an attractive response to some of these concerns in the algorithmic accountability space, but it risks being conflated with democratic control. More likely, however, its ability to be mainstreamed into a procedural audit requirement provides legitimacy to the tech industry to continue developing AI as it has been and undercuts calls for regulation, while asking for even greater resources from those impacted to ensure the accountability of the firms responsible for creating harm.

## "Access to data" as a weak policy response given the shrinking space for independent research

Provisions mandating data access for vetted researchers are being integrated into a growing number of policy proposals. Given the way many platforms mediate key domains of society and how obscure the inner workings of decision-making algorithms are, granting access to platform data is both needed and societally beneficial. This research should be protected under robust safe-harbor provisions that provide good-faith researchers with immunity from legal charges associated with hacking:[157] in particular, the question of whether research that involves web scraping, a practice researchers are forced to rely on when companies refuse to share their data, is legal under the Computer Fraud and Abuse Act (CFAA),[158] a question that is still being litigated.[159] Web scraping should receive robust protections under the law.[160] Additionally, community-based research offers a meaningful and robust means through which to shift the balance of power away from company-directed approaches to accountability. This research deserves not only strong legal protections and access, but the adequate resourcing to enable communities to document harms.

**However, data access provisions can be harmful when they are used to supplant other structural remedies. This implicitly shifts the burden away from companies and onto under-resourced actors for identifying tech-enabled harms. It also puts platforms in a gatekeeping position over tech accountability work.**

Policy proposals, including the US Platform Accountability and Transparency Act and the EU Digital Services Act, position data access as a stand-in for other forms of accountability. This

[155] Note that GOP leaders and the US Chamber of Commerce have both been supportive of the NIST RMF approach. See for example Nihal Krishan, "GOP House Committee Leaders Probe 'Conflicting Definitions' in NIST AI Framework and AI 'Bill of Rights'," FedScoop, January 27, 2023; and LaCasse, "US NIST publishes AI Risk Management Framework 1.0."

[156] This question may be posed of auditing frameworks more broadly. See for example Michael Power, *The Audit Society: Rituals of Verification* (Oxford: Oxford University Press, 1997; see also remarks by Arvind Narayanan, Federal Trade Commission, "PrivacyCon 2022: Part 1," video.

[157] Alex Abdo, Ramya Krishnan, Stephanie Krent, Evan Welber Falcón, and Andrew Keane Woods, "A Safe Harbor for Platform Research," Knight First Amendment Institute at Columbia University, January 19, 2022.

[158] Christian W. Sandvig et al. v. Loretta Lynch, United States District Court for the District of Columbia, Case 1:16-cv-1368 (JDB), October 7, 2016.

[159] American Civil Liberties Union, "Sandvig v. Barr — Challenge to CFAA Prohibition on Uncovering Racial Discrimination Online," May 22, 2019.

[160] Rachel Goodman, "Tips for Data Journalism in the Shadow of an Overbroad Anti-Hacking Law," American Civil Liberties Union, October 13, 2017.

presumes the existence of a robust and well-resourced body of researchers with ample time, resources, and expertise to conduct meaningful technical audits. This is far from the reality, and it benefits companies to promote this positioning since it removes responsibility for the safety of their products from their hands.[161]

Such proposals also grant platforms the opportunity to act as gatekeepers over potentially critical research in multiple ways[162]:

- Through who gets granted access to data, in particular through narrow interpretations of the definition of "research" and "researcher" that may exclude investigative journalists and civil society advocates[163]
- Through claims that certain research raises "feasibility concerns" or creates an undue burden for the company, and thus must be blocked from access, or by immunizing them against certain causes of action in exchange for the provision of data[164]
- Through prior review before publication of research based on data access: companies may claim trade secrecy over the insights contained in critical research papers and ensure they never see the light of day[165]

Lastly, these proposals need to be read in the context of an increasingly precarious environment for critical tech accountability research, in which economic pressure leaves academic researchers increasingly exposed to undue influence by corporate actors.[166]

[161] This also, as a report by the Center for Democracy and Technology notes, grants an opening for law enforcement agencies to utilize data access provisions to step up their demands for platform information. See Caitlin Vogus, "Report – Defending Data: Privacy Protection, Independent Researchers, and Access to Social Media Data in the US and EU," Center for Democracy and Technology, January 25, 2023.

[162] In August 2021, Meta disabled the accounts of researchers at NYU's Ad Observatory who were investigating political ads and the spread of misinformation on Facebook. See Meghan Bobrowsky, "Facebook Disables Access for NYU Research into Political-Ad Targeting," *Wall Street Journal*, August 4, 2021; Cristiano Lima, "Twitter Curbs Researcher Access, Sparking Backlash in Washington," *Washington Post*, February 3, 2023; and Mike Clark, "Research Cannot Be the Justification for Compromising People's Privacy," Meta, August 3, 2021.

[163] For example, under the DSA researchers must be "vetted" and (1) be affiliated with an academic institution (2) be independent from commercial interests, (3) have proven records of expertise in the fields related to the risks investigated or related research methodologies, and (4) commit to and be in a capacity to preserve data security and confidentiality requirements.

[164] Platform Accountability and Transparency Act, 117th Congress (2021–2022), First Session.

[165] Georgia Wells, Jeff Horwitz, and Deena Seetharaman, "Facebook Knows Instagram Is Toxic for Teen Girls, Company Documents Show," *Wall Street Journal*, September 14, 2021.

[166] See J. Nathan Matias, Susan Benesch, Rebekah Tromble, Alex Abdo, J. Bob Alotta, David Karpf, David Lazer, Nathalie Maréchal, Nabiha Syed, and Ethan Zuckerman, "Manifesto: The Coalition for Independent Technology Research," Coalition for Independent Technology Research, October 12, 2022; and "Gig Economy Project – Uber whistleblower Mark MacGann's full statement to the European Parliament," Brave New Europe, October 25, 2022.

Spotlight

# Data Minimization as a Tool for AI accountability

Broad data minimization principles (“collect no more data than necessary”), a core part of data privacy laws like the EU’s GDPR, have been woefully underenforced and given too much interpretive wiggle room.

But the next generation of data minimization policies—bright-line rules that prohibit excessive or harmful data collection and use—show greater promise. Championed by a growing chorus within civil society, these data rules could be a powerful lever in restraining some of the most concerning AI systems (and even the business model that sustains them).

**Broad data minimization principles (“collect no more data than necessary”) are a core part of global data privacy laws like the GDPR, but have been woefully underenforced.**

Data privacy policy approaches have evolved considerably over the past decade. The abject failure of the “notice and consent” model—which mandates that data collection is broadly permissible provided the user has been notified and given consent—as the primary way to protect people’s privacy is now a mainstream critique.[167] The dominant legal privacy regime globally, led by the European GDPR, retains

[167] See Federal Trade Commission, “Trade Regulation on Commercial Surveillance and Data Security,” 16 CFR Part 464, 2022, https://www.ftc.gov/system/files/ftc_gov/pdf/commercial_surveillance_and_data_security_anpr.pdf; Neil Richards and Woodrow Hartzog, “The Pathologies of Digital Consent,” Washington University Law Review 96, no. 6 (2019), https://openscholarship.wustl.edu/cgi/viewcontent.cgi?article=6460&context=law_lawreview; and Claire Park, “How ‘Notice and Consent’ Fails to Protect Our Privacy,” New America (blog), March 23, 2020, https://www.newamerica.org/oti/blog/how-notice-and-consent-fails-to-protect-our-privacy.

consent as a way to legitimize data processing in certain instances but also imposes baseline standards on firms' data processing activities that apply irrespective of what the user "chooses."[168]

*Data minimization* is the umbrella term increasingly used to refer to some of these core obligations. Aimed at limiting the incentives for unbridled commercial surveillance practices, these include (1) restrictions on what data is collected (collection limitations), (2) the purposes for which it can be used following collection (purpose limitations), and (3) the amount of time firms can retain data (storage limitations).[169] These rules require firms to demonstrate the necessity and proportionality of the data processing—to prove, for example, that it is in fact necessary to collect certain kinds of data for the purposes they seek to achieve; or to state that they will only use such data for predefined purposes; or to ensure that they will only retain data for a period of time that is necessary and proportionate to these purposes. Typically, certain types of data classified as "sensitive" receive a heightened level of protection, for example, a stricter standard of necessity for the collection of biometric data with fewer exceptions.[170] In the US, data minimization rules are a part of the California Privacy Rights Act,[171] which came into force in January 2023 and is also a core part of a proposed federal privacy law, the American Data Privacy and Protection Act, that has gained widespread momentum.[172]

These broad data-minimization principles offer a clear shift away from consent or control-based approaches. They shift the burden away from individuals having to make decisions or proactively exercise their data rights, and onto firms to demonstrate their compliance with these principles in the interests of users.[173] They also create clear curbs on the kinds of invasive data processing companies are otherwise incentivized to engage in under the behavioral advertising business model.

Despite their strong potential, in practice, these standards (now a part of data protection laws like the GDPR and more than a hundred counterparts around the world)[174] haven't had the kind of structural impact they promise. A key reason for this is the inherent ambiguity in interpreting the legal standards of necessity and proportionality encoded in these principles,[175] which, combined with overburdened enforcement agencies,[176] leaves companies a great deal of leeway in how to apply (or likely evade) these requirements. The enforcement of data minimization throws up fundamentally thorny questions: *Does maximizing advertising revenue qualify as a reasonable business purpose? If so, does it justify virtually*

[168] Intersoft Consulting, "Art. 5 GDPR: Principles Relating to Processing of Personal Data," n.d., accessed March 3, 2023, https://gdpr-info.eu/art-5-gdpr.

[169] Ibid. See also "Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the Protection of Natural Persons with Regard to the Processing of Personal Data by the Union Institutions, Bodies, Offices and Agencies and on the Free Movement of Such Data, and Repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC," *Official Journal of the European Union*, November 21, 2018, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018R1725; and https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/data-minimisation.

[170] See Intersoft Consulting, "Art. 9 GDPR: Processing of Special Categories of Personal Data," n.d., accessed March 15, 2023, https://gdpr-info.eu/art-9-gdpr; and Information Commissioner's Office (ICO), "What Are the Rules on Special Category Data?" n.d., accessed March 15, 2023, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/special-category-data/what-are-the-rules-on-special-category-data.

[171] "California Consumer Privacy Act (CCPA)," Rob Bonta, Attorney General, State of California Department of Justice, February 15, 2023, https://oag.ca.gov/privacy/ccpa.

[172] American Data Privacy and Protection Act, H.R. 8152, 117th Congress (2021–2022) https://www.congress.gov/bill/117th-congress/house-bill/8152/text.

[173] David Medine and Gayatri Murthy, "Companies, Not People, Should Bear the Burden of Protecting Data," Brookings Institution, December 18, 2019, https://www.brookings.edu/blog/techtank/2019/12/18/companies-not-people-should-bear-the-burden-of-protecting-data.

[174] Graham Greenleaf, "Global Data Privacy Laws 2019: 132 National Laws & Many Bills," *Privacy Laws & Business International Report* 157 (2019), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3381593.

[175] See Josephine Wolff and Nicole Atallah, "Early GDPR Penalties: Analysis of Implementation and Fines through May 2020," *Journal of Information Policy* 11 (December 2021), https://scholarlypublishingcollective.org/psup/information-policy/article/doi/10.5325/jinfopoli.11.2021.0063/291999/Early-GDPR-Penalties-Analysis-of-Implementation; and Information Commissioner's Office (ICO), *Big Data, Artificial Intelligence, Machine Learning and Data Protection*, September 4, 2017, https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf.

[176] Access Now, "Access Now Raises the Alarm over Weak Enforcement of the EU GDPR on the Two-Year Anniversary," press release, May 25, 2020, https://www.accessnow.org/alarm-over-weak-enforcement-of-gdpr-on-two-year-anniversary.

*limitless data collection for behavioral advertising? How far can security justifications stretch to legitimize indefinite data retention?* These issues are far from resolved despite almost a decade of enforcement. There have been far and few notable exceptions where data minimization principles in the GDPR have been enforced to successfully draw bright-line rules against certain kinds of data processing. In one example, the Swedish Data Protection Authority outlawed the use of facial recognition in schools on the basis of the collection limitation principle, finding that its use for monitoring attendance was a disproportionate means to achieve this goal.[177]

### A range of new data minimization proposals move toward specific restrictions around excessive or harmful data practices, such as restricting targeted advertising or banning the collection of biometric data in certain domains.

A new iteration of data-minimization rules could overcome these challenges by moving beyond high-level normative standards (as in the GDPR) to specific restrictions around particular types of data and kinds of data use. Bold proposals have been surfaced in the US by civil society and in legislative proposals, including restricting the use of data for targeted advertising,[178] or a narrower version that limits the use of sensitive data for all secondary purposes, including advertising;[179] restricting the collection and use of biometric information for particular groups such as children;[180] and in certain contexts such as workplaces, schools, and hiring.[181]

These proposals clarify bright-line rules when it comes to data collection and use. Some, like the ban on using data for behavioral advertising, are justified as both pro-privacy and pro-competition interventions since they target first-party data collection that is currently concentrated among Big Tech companies.[182] (See also: Toxic Competition**)**

The proposals also could effectively shut down some of the most concerning uses of AI—for example, by placing restrictions on the collection of emotion-related data or restricting biometric data collection in the workplace (which fuels a range of algorithmic surveillance and management tools). In these ways,

[177] European Data Protection Board, "Swedish DPA: Police Unlawfully Used Facial Recognition App," February 12, 2021, https://edpb.europa.eu/news/national-news/2021/swedish-dpa-police-unlawfully-used-facial-recognition-app_en.

[178] See Accountable Tech, "Accountable Tech Petitions FTC to Ban Surveillance Advertising as an 'Unfair Method of Competition'," press release, September 28, 2021, https://accountabletech.org/media/accountable-tech-petitions-ftc-to-ban-surveillance-advertising-as-an-unfair-method-of-competition; Electronic Privacy Information Center (EPIC) and Consumer Reports, *How the FTC Can Mandate Data Minimization through a Section 5 Unfairness Rulemaking*, January 2022, https://epic.org/documents/how-the-ftc-can-mandate-data-minimization-through-a-section-5-unfairness-rulemaking; Accountable Tech, "Ban Surveillance Advertising: Coalition Letter," 2022, accessed March 15, 2023, https://www.bansurveillanceadvertising.com/coalition-letter; and *In the Matter of Trade Regulation Rule on Commercial Surveillance and Data Security, R111004, Before the Federal Trade Commission, Washington, D.C.*, November 21, 2022 (statement of Center for Democracy & Technology), https://cdt.org/wp-content/uploads/2022/11/CDT-Comments-to-FTC-on-ANPR-R111004.pdf.

[179] Ada Lovelace Institute, *Countermeasures: The Need for New Legislation to Govern Biometric Technologies in the UK*, June 2022, https://www.adalovelaceinstitute.org/wp-content/uploads/2022/06/Countermeasures-the-need-for-new-legislation-to-govern-biometric-technologies-in-the-UK-Ada-Lovelace-Institute-June-2022.pdf.

[180] Ban Facial Recognition Technologies for Children—and for Everyone Else", 26 B.U. J. S CI . & T ECH . L. 223 (2020)

[181] See Worker Rights: Workplace Technology Accountability Act, A.B. 1651, California Legislature (2021–2022), https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202120220AB1651; Sofia Edvardsen, "How to Interpret Sweden's First GDPR Fine on Facial Recognition in School," International Association of Privacy Professionals (IAPP), August 27, 2019, https://iapp.org/news/a/how-to-interpret-swedens-first-gdpr-fine-on-facial-recognition-in-school; European Data Protection Board, "EDPB & EDPS Call for Ban on Use of AI for Automated Recognition of Human Features in Publicly Accessible Spaces, and Some Other Uses of AI That Can Lead to Unfair Discrimination," June 21, 2021, https://edpb.europa.eu/news/news/2021/edpb-edps-call-ban-use-ai-automated-recognition-human-features-publicly-accessible_en; and "When Bodies Become Data: Biometric Technologies and Free Expression," Article 19, April 2021, https://www.article19.org/biometric-technologies-privacy-data-free-expression.

[182] Accountable Tech, "FTC Rulemaking Petition to Prohibit Surveillance Advertising," 2022, accessed March 15, 2023, https://accountabletech.org/campaign/ftc-public-comment.

the next generation of data minimization rules could be a powerful lever in addressing some of the most concerning AI systems and the business model that sustains them.

Algorithmic Management

# Creating Bright-Line Rules to Restrain Workplace Surveillance

To meaningfully build worker power, we must create policies to regulate algorithmic management that confront why workplace surveillance is particularly harmful: because algorithmic systems are used to justify unfair decisions that impact workers' pay, safety, and access to resources, because they are invasive of workers' private lives, and because they inhibit workers' ability to organize.

There is a clear case for bright-line rules that restrain the use of these tools altogether and at minimum create no-go zones around the most invasive forms of surveillance. Such a policy regime could help even out the power imbalances between workers, employers, and the companies that sell these tools.

**Algorithmic management is on the rise. Worker-led organizing over the past several years has called attention to how algorithmic management ratchets up the devaluation of work, leads to the deterioration of working conditions and creates risks to workers' health and safety,[183] unequally distributes risks and privileges, threatens protected worker-led collective action, and leads to the destruction of individual and worker privacy.[184] Policy responses must attend to these calls by confronting the pace and scale of this ramp-up in ways that are attuned to upholding workers' wages, privacy, autonomy and their right to engage in collective action.[185]**

Surveillance of workers and workplaces has ramped up since the start of the pandemic, spurred by the shift to remote work, an increased blurring of work and home, and the integration of workplace technology into personal devices and spaces.[186] While this is occurring across industries and levels of management,[187] low-wage workers have been at the forefront of the fight to end workplace surveillance and algorithmically-enabled harms. Worker-led organizing brought attention to how algorithmic management is being used for such things as setting workers' benchmarks and pay,[188] setting productivity quotas,[189] and making recommendations to hire, promote, demote, and fire workers.[190]

Companies give many disparate reasons for why they deploy surveillance tech at work, making weakly supported claims that they curb discrimination, offer metrics useful for mid-tier management to demonstrate compliance, and increase the efficiency of certain labor-intensive processes like reading through applicant resumes. But their deleterious effects far outweigh these justifications: algorithmic management ratchets up the devaluation of work, unequally distributes risks and privileges, threatens protected worker-led collective action, and leads to the destruction of individual and worker privacy.[191]

[183] Edward Ongweso Jr, "Amazon's New Algorithm Will Set Workers' Schedules According to Muscle Use", Vice, April 15, 2021; WWRC, "The Public Health Crisis Hidden in Amazon Warehouses", *WWRC*, January 14, 2021; Strategic Organizing Center, "Safety and Health at Amazon Campaign", *Strategic Organizing Center*; Strategic Organizing Center, "The Injury Machine: How Amazon's Production System Hurts Workers," *Strategic Organizing Center*, April 2022; Strategic Organizing Center, "The Worst Mile: Production Pressure and the Injury Crisis in Amazon's Delivery System", *Strategic Organizing Center*, May 2022.

[184] See Athena, "Put Workers over Profits: End Worker Surveillance", *Medium*, October 14, 2020; Sara Machi, "'We are not robots' Amazon workers in St. Peters join international picket on Black Friday", *ksdk*, November 25, 2022; Athena, Letter to FTC on Corporate Surveillance, *Medium*, July 29, 2021. Aloisi and De Stefano, *Your Boss is an Algorithm: Artificial Intelligence, Platform Work and Labour* (Oxford: Hart Publishing); Karen Levy, *Data Driven: Truckers, Technology and the New Workplace Surveillance* (Princeton: Princeton University Press, 2023); Pauline Kim, "Data-Driven Discrimination at Work," *William & Mary Law Review* 48 (2017): 857–936; and Miranda Bogen and Aaron Rieke, "Help Wanted: An Examination of Hiring Algorithms, Equity, and Bias," Upturn, December 2018.

[185] Jeremias Adams-Prassl, Halefom H. Abraha, Aislinn Kelly-Lyth, M. Six Silberman, Sangh Rakshita, "Regulating Algorithmic Management: A Blueprint", March 1, 2023.

[186] See Jodi Kantor and Arya Sundaram, "The Rise of the Worker Productivity Score," *New York Times*, August 14, 2022; Sissi Cao, "Amazon Unveils AI Worker Monitoring For Social Distancing, Worrying Privacy Advocates," *Observer*, June 16, 2020; Zoë Corbyn, "'Bossware Is Coming for Almost Every Worker': The Software You Might Not Realize Is Watching You," *Guardian*, April 27, 2022; Irina Ivanova, "Workplace Spying Surged in the Pandemic. Now the Government Plans to Crack Down," CBS News, November 1, 2022; and Danielle Abril and Drew Harwell, "Keystroke Tracking, Screenshots, and Facial Recognition: The Boss May Be Watching Long After the Pandemic Ends," *Washington Post*, September 24, 2021.

[187] Such techniques have a long history, though what we see at present is an acceleration of these long-standing trends. See for example Min Kyung Lee, Daniel Kusbit, Evan Metsky, and Laura Dabbish, "Working with Machines: The Impact of Algorithmic and Data-Driven Management on Human Workers," CHI '15: Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems (April 2015): 1603–1612; Wilneida Negrón, "Little Tech Is Coming for Workers: A Framework for Reclaiming and Building Worker Power," Coworker.org, 2021; Antonio Aloisi and Valerio De Stefano, *Your Boss Is an Algorithm: Artificial Intelligence, Platform Work and Labour* (Oxford: Hart Publishing: 2022); Alexandra Mateescu and Aiha Nguyen, "Algorithmic Management in the Workplace," Data & Society, February 2019; Richard A. Bales and Katherine V.W. Stone, "The Invisible Web at Work: Artificial Intelligence and Electronic Surveillance in the Workplace," *Berkeley Journal of Employment & Labor Law* 41, no. 1 (2020): 1–62; Ifeoma Ajunwa, Kate Crawford, and Jason Schultz, "Limitless Worker Surveillance," *California Law Review* 105, no. 3 (June 2017): 101–142; and Kirstie Ball, "Electronic Monitoring and Surveillance in the Workplace: Literature Review and Policy Recommendations," Joint Research Centre (European Commission), November 15, 2021.

[188] Tracey Lien, "Uber class-action lawsuit over how drivers were paid gets green light from judge", *Los Angeles Times*, February 19, 2018.

[189] Albert Samaha, "Amazon Warehouse Worker Daniel Olayiwola Decided to Make a Podcast About Amazon's Working Conditions", *Buzzfeed*, February 16, 2023, https://www.buzzfeednews.com/article/albertsamaha/daniel-olayiwola-amazon-scamazon-podcast.

[190] Rideshare Drivers United (RDU) and Asian Americans Advancing Justice - Asian Law Caucus (ALC), "Fired By An App: The Toll of Secret Algorithms and Unchecked Discrimination on California Rideshare Drivers", Asian Americans Advancing Justice - Asian Law Caucus, February 28, 2023.

[191] See Aloisi and De Stefano, *Your Boss is an Algorithm*; Karen Levy, *Data Driven: Truckers, Technology and the New Workplace Surveillance* (Princeton: Princeton University Press, 2023); Pauline Kim, "Data-Driven Discrimination at Work," *William & Mary Law Review* 48 (2017): 857–936; and Miranda Bogen and Aaron Rieke, "Help Wanted: An Examination of Hiring Algorithms, Equity, and Bias," Upturn, December 2018.

What worker-driven efforts underscore is that workplace surveillance has little to do with productivity, efficiency, or safety: fundamentally, these systems are designed for control.

To understand how algorithmic management, worker surveillance, and Big Tech function in concert, we need to interpret them through the same analysis: the ability to leverage information as a source of power.[192] This is as true in the employer-employee relationship as it is of the power imbalance between tech firms and their users. And in both cases, those with access and control over information accrue benefits at the cost of worker rights, autonomy and dignity. The right path forward is to institute meaningful curbs on surveillance and algorithmic control in workplace settings that rebalance the power discrepancy between workers and employers by upholding worker autonomy and the right to engage in collective action.[193]

## Labor Technology Policy: Principles of The Emerging Framework

Worker-specific surveillance concerns are starting to get more policy attention in the US and EU. The newly unveiled Stop Spying Bosses Act would mandate disclosures and institute prohibitions on the collection of data on workers, and would establish a Privacy and Technology Division at the Department of Labor devoted to the regulation and enforcement of workplace surveillance technologies.[194] The proposed EU Platform Work Directive would afford baseline protections to improve conditions for platform workers, including mandates for worker access to data, algorithmic transparency, and contestability.[195] A proposed California Workplace Technology Accountability Act would create bright-line rules around certain types of algorithmic management and worker surveillance, and includes mandates for impact assessments and transparency measures.[196] The White House-issued Blueprint for an AI Bill of Rights indicates that the enumerated rights should extend to all employment-related systems, including workplace algorithms and workplace surveillance and management systems.[197] And the US National Labor Relations Board has expressed concerns that employers' expanded ability to monitor and manage employees may create potential interference with employees' ability to engage in protected activity and keep that activity confidential from their employer.[198] This growing interest is coalescing around an emerging framework for labor technology policy.

[192] Matthew Bodie, "Beyond Privacy: Changing The Data Power Dynamics In The Workplace", *LPE Project*, July 2, 2023.
[193] Jeremias Adams-Prassl, Halefom H. Abraha, Aislinn Kelly-Lyth, M. Six Silberman, Sangh Rakshita, "Regulating Algorithmic Management: A Blueprint", March 1, 2023.
[194] Bob Casey, Cory Booker, and Brian Schatz, "Stop Spying Bosses Act of 2023."
[195] European Commission, "Commission Proposals to Improve the Working Conditions of People Working Through Digital Labour Platforms," press release, December 9, 2021.
[196] Worker Rights: Workplace Technology Accountability Act, A.B. 1651, California Legislature (2021–2022).
[197] White House, Office of Science and Technology Policy (OSTP), "Blueprint for an AI Bill of Rights," October 2022, 3.
[198] See Jennifer A. Abruzzo, National Labor Relations Board General Counsel, "Memorandum GC 23-02," October 31, 2022.The concerns outlined in Abruzzo's memo are backed by well-documented evidence; see for example Ari Shapiro, "Amazon Reportedly Has Pinkerton Agents Surveil Workers Who Try to Form Unions," NPR, November 30, 2020.

**Worker-surveillance policy proposals in the US must bolster collective organizing and collective bargaining. This should underscore the right of workers to engage in protected concerted activity:[199] all workers deserve protection from algorithmic management and workplace surveillance.**

While the breadth of proposals is a promising signal, these frameworks need to do more to address power relationships in the labor context, and to tie protections to fundamental rights to autonomy, collective organizing, and collective bargaining. Such frameworks should necessarily remain distinct from, though supportive of, more traditional models of business unions. All workers deserve protection from algorithmic management and workplace surveillance, regardless of whether they are currently members of unions or become union members in the future. Given that these systems impact workers across sectors and at all levels of management, such protections should be broad-based, extending beyond platform-based work to encompass all industry verticals and to include managers. They should include robust whistleblower protections given both the importance of whistleblowing to surfacing tech-enabled harms and the clear pattern of retaliation against workers who do so.[200] They should include enforcement of existing domains of law to algorithmic management systems, such as using workplace safety laws to curb algorithmic systems that are increasing worker injury rates and labor laws to address just-in-time shift scheduling algorithms that may violate wage and hour laws.[201] Lastly, they should provide for collective, not just individual, rights given their importance to worker-led organizing as a core mode of tech accountability.

## Worker Organizing and Tech Policy

Tech worker organizing has proven one of the most effective and direct means to curbing tech-enabled harms before they occur. Workers have taken significant risks to engage in collective action, blowing the whistle on harmful technologies and contractual agreements while still in the development. They have also been markedly successful in convincing their employers to drop contracts with military agencies, calling out human rights violations, and agitating for better workplace conditions and worker protections.

Many of those on the frontlines of this work have experienced retaliation of many kinds. It is for this reason that achieving strong baseline labor protections, including stronger whistleblower protections, is centrally relevant to all domains of tech policy: an accountable, ethical, responsible, and justice-oriented tech sector will only be built upon a base of organized worker power.

Worker-led pushback faces headwinds on many fronts: the industry is retrenching, instituting layoffs while preserving executive compensation. Even before the current economic climate, tech companies took retaliatory measures against their most vocal internal critics, firing many members of the initial wave of tech worker organizing. Already among the world's most surveillant companies, tech firms closely monitor workers' activities: Amazon went as far as to hire Pinkerton

[199] National Labor Relations Board, "Concerted Activity," n.d., accessed March 3, 2023.

[200] Athena, "Silencing of Whistleblowers in the Workplace is a Threat to Public Health", *Medium*, May 1, 2020; Lauren Kaori Gurley, "Amazon Warehouse Workers in Minnesota Walk Off the Job, Protest Alleged Retaliation", *Vice*, October 2, 2020.

[201] AFL-CIO Technology Institute, "Woodall AFL-CIO Tech Institute Digital Trade Testimony", November 30, 2022.

operatives - the same private security firm infamously known for union-busting during the 19th and early 20th centuries - to spy on warehouse workers, labor organizers and environmental activists.

This is why policy measures that bolster worker organizing are also key to curbing concentrated power in the tech industry, such as strengthening whistleblower protections, establishing strong curbs on non-disclosure and non-disparagement agreements, and barring employers from using non-compete clauses.

### Transparency and data-access measures are necessary but insufficient; the burden should be placed on developers and employers rather than on those harmed by it.

Workplace surveillance is particularly harmful given its opacity. It extends employers' power over workers and expands the scope of their gaze into the most intimate corners of workers' lives. To counter this expanded information asymmetry, many proposals for worker data rights regimes focus on transparency and mandated disclosures around the use of algorithmic systems and surveillance in the workplace as a baseline accountability measure.[202] This includes the ways in which workplace surveillance systems are used, their parameters, their data inputs, and their methods of deployment. The goal of these "worker data rights" proposals is to even out the information asymmetries that exist between workers and employers, and in particular to account for the increased power employers gain through the more invasive collection of data enabled by algorithmic systems. The proposals seek to ensure that workers know what kind of data is being collected about them and how it will be used, and that they have a right to access and correct flawed or incorrect data, as well as to contest decisions made about them unfairly.

The strongest of these proposals dig deeply into the details, mandating that disclosures take place in multiple phases, including prior to the deployment of a system. They also acknowledge explicitly that consent is not a meaningful framework in the context of work, heading off at the pass any presumption that knowledge of a system is tantamount to acceptance of its use given the risk that refusal to use a work-mandated system could lead to retaliation.[203]

While transparency may help balance out information asymmetries that benefit employers, proposed worker data rights regimes otherwise fall short in many ways. First, such policy frameworks fail to grapple with the relationships between workers, employers, and the vendors who provide the software used for algorithmic management and workplace surveillance—who gains power through the deployment of these systems and who loses it. Telling workers that their employer has used algorithmic targeting to systematically lower their wages is no substitute for enacting rules to ensure wages are set fairly and at amounts workers can live on in the first place. And through contractual obligations and claims to trade secrecy, both employers and software vendors are incentivized to resist mandates that

[202] UC Berkeley's Labor Center has a robust compilation of policy information about the case for worker technology rights; see Annette Bernhardt, Reem Suleiman, and Lisa Kresge, "Data and Algorithms at Work," UC Berkeley Labor Center, November 3, 2021.
[203] One example is the use of AI-powered hiring software. While developments such as Illinois' Artificial Intelligence Video Interview Act (2020) and New York City's Local Law 144 compel employers to inform candidates when they are being processed by an AI-powered tool and offer them a viable alternative, candidates may be unwilling to ask for an alternative lest they be seen as a "difficult" or noncompliant candidate. See Illinois General Assembly, "Artificial Intelligence Video Interview Act," 820 ILCS 42/, 2021; and New York City Council, "Automated Employment Decision Tools," 2021/144.

require them to provide full access to workers' data.[204] Even when all parties are willing to make access available to workers, where to locate the data, and the models trained on it, still present challenging organizational problems that employers may claim they cannot fulfill.[205]

Second, policy frameworks that emphasize data access are premised on the existence of external actors who have adequate resources and capacity to make sense of the data. While many groups are rising to meet this need,[206] it's often the case that those with the context and expertise needed to parse through sometimes staggering amounts of data—workers themselves and their elected representatives, investigative journalists, researchers, and civil society groups—have comparatively fewer resources and time to contribute to such tasks. Moreover, knowledge of harmful corporate practices is not tantamount to asserting power or control over them, but only a first step.[207] Thus inherent information and power asymmetries must be taken into account as the precondition for any future policy framework—ultimately an approach that utilizes bright-line rules that clearly limit abusive practices would place the onus on those that benefit from algorithmic management, rather than overburdening those who are most likely to be harmed with additional work.

### We must establish clear red lines around domains and types of technology that are inappropriate for use in any instance.

Many policy proposals addressing algorithmic management include red lines that establish domains and types of technology that should never be deployed in a workplace context:

- Clear red lines should be established around obvious private areas that an employer has no right to monitor, such as office bathrooms and employees' cars.[208]
- There should be boundaries around an employee's functional time, such that monitoring by an employer does not extend into off-duty hours, though in many job contexts this boundary is blurry.[209]
- Certain types of technology, such as emotion recognition, should be prohibited under policy frameworks from being used in an employment context, both because these systems are pseudoscientific[210] and because it is inappropriate for an employer to attempt to ascertain a worker's inner psychological state.[211]
- Harmful practices such as algorithmic wage discrimination should be banned outright.[212]

[204] See for example Worker Info Exchange, "Managed by Bots: Data-Driven Exploitation in the Gig Economy," December 2021.

[205] See Will Evans, "Amazon's Dark Secret: It Has Failed to Protect Your Data," *Wired*, November 18, 2021; Information Commissioner's Office (ICO), "Principle (e): Storage limitation," n.d., accessed March 3, 2023; and Intersoft Consulting, "Art. 5 GDPR: Principles Relating to Processing of Personal Data," n.d., accessed March 3, 2023.

[206] See for example Worker Info Exchange; Massachusetts Institute of Technology School of Architecture + Planning, "The Shipt Calculator: Crowdsourcing Gig Worker Pay Data to Audit Algorithmic Management"; and Alex Pentland and Thomas Hardjono, "Data Cooperatives," April 30, 2020.

[207] Veena Dubal, "On Algorithmic Wage Discrimination," *SSRN,* January 23, 2023; Zephyr Teachout, "Personalized Wages", *SSRN,* May 12, 2022.

[208] Worker Rights: Workplace Technology Accountability Act, A.B. 1651.

[209] See Worker Rights: Workplace Technology Accountability Act, A.B. 1651; and European Commission, "Proposal for a Directive of the European Parliament and of the Council on Improving Working Conditions in Platform Work," December 9, 2021.

[210] See Information Commissioner's Office (ICO), "'Immature Biometric Technologies Could Be Discriminating against People' Says ICO in Warning to Organisations," October 26, 2022; Worker Rights: Workplace Technology Accountability Act, A.B. 1651; and Ifeoma Ajunwa, "Automated Video Interviewing as the New Phrenology," *Berkeley Technology Law Journal* 36, no. 3 (October 2022): 1173–1226.

[211] See European Commission, "Proposal for a Directive of the European Parliament and of the Council on Improving Working Conditions in Platform Work."

[212] See Dubal, "On Algorithmic Wage Discrimination."

Purpose limitations and prohibitions on secondary use, such as prohibitions on the sale or licensing of worker data to third parties,[213] are included in many policy proposals that target algorithmic management practices.[214] These serve as an important curb on what the scholar Karen Levy describes as *surveillance interoperability*, or the mutual reinforcement of worker surveillance through the combination of government data collection, corporate surveillance, and third-party data harvesting.[215] Workers are exposed to multiple and reinforcing surveillance regimes, and information collected about them in one context can be relatively easily ported to another - for example, companies like Argyle advertise themselves as data brokers for employment data, combining data streams from many sources to provide services such as 'risk assessments' about rideshare drivers for insurers.[216] Others, like Appriss Retail, combine data sources such as point of sale transaction data with criminal background information to help retail managers evaluate the risk of any given employee committing fraud.[217] Such systems are riddled with flaws and offer little transparency or recourse to workers when they make what are often consequential mistakes.[218]

For this reason, curbing these practices requires both placing clear limits on data collection, and ensuring that data (and any models trained on it) cannot have a second life by being ported to another context. These measures could be further complemented through proposed changes to competition law that would inhibit tech firms' ability to combine streams of data across their many holdings (See also: Toxic Competition).

In comparison to proposals that center data rights and data access, proposals that put forth bright lines and purpose limitations as an enforcement tool will be much more effective at pursuing accountability for the use of algorithmic systems in a workplace context. However, challenges remain around establishing clear definitions, such defining the boundary between work and home, in ways that reflect the lived experience of workers—particularly with the increase in remote work, as well as the use of personal technology devices for work practices.[219]

### "Human in the loop" policy proposals operate from a flawed perspective on how algorithmic management works in practice and fail to provide meaningful accountability.

Many proposals outline a subset of activities that should be constrained from being fully automated due to the significance of the decision-making involved: these include hiring, promotion, termination, and discipline of workers.[220] Some proposals extend this list to any effect of an algorithmic system that has an impact on working conditions, requiring regular review of potential impacts, particularly where they are likely to effect health and safety. These "human in the loop" proposals coalesce around

[213] See Worker Rights: Workplace Technology Accountability Act, A.B. 1651; and Lora Kelley, "What Is 'Dogfooding'?" *New York Times*, November 14, 2022.
[214] Jeremias Adams-Prassl, Halefom H. Abraha, Aislinn Kelly-Lyth, M. Six Silberman, Sangh Rakshita, "Regulating Algorithmic Management: A Blueprint", March 1, 2023.
[215] Karen Levy, "Labor under Many Eyes: Tracking the Long-Haul Trucker," Law and Political Economy (LPE) Project, January 31, 2023.
[216] Argyle.
[217] Appriss Retail.
[218] See Negron, "Little Tech Is Coming For Workers"
[219] See Aiha Nguyen and Eve Zelickson, "At the Digital Doorstep: How Customers Use Doorbell Cameras to Manage Delivery Workers," Data & Society, October 2022; Gabriel Burdin, Simon D. Halliday, Fabio Landini, "Why Using Technology to Spy on Home-Working Employees May Be a Bad Idea," London School of Economics, June 17, 2020; Personnel Today, "Technology blurs boundaries between work and home for 'Generation Standby'," May 20, 2010.
[220] See Worker Rights: Workplace Technology Accountability Act, A.B. 1651; and European Commission, "Proposal for a Directive of the European Parliament and of the Council on Improving Working Conditions in Platform Work."

requiring human review of proposed decisions through an algorithmic system, and many also require a right to reversal if a decision is made incorrectly or unfairly.

The framing of these proposals elides the reality that decisions made using AI systems are rarely ever fully automated or fully human, but generally lie on a continuum between the two. Furthermore, incorporating a human operator can actually legitimize, rather than provide protection against, flawed or opaque decision-making via automated systems. Adding a human to the loop may "rubber-stamp" automated decisions rather than increase their nuance and precision.[221] There is no clear definition of what would constitute "meaningful" oversight, and research indicates that people presented with the advice of automated tools tend to exhibit automation bias, or deference to automated systems without scrutiny.[222] Lastly, such proposals can lead to a blurring of responsibility, in which the person responsible for human oversight is blamed for systemic failures over which they have little control.[223] These weaknesses need to be accounted for through greater scrutiny of human oversight mechanisms and by addressing tensions around whether algorithms should be involved in certain decisions at all through bright-line measures.

### Audits may offer tech companies and employers opportunities to mischaracterize their practices, and imply they can be contested when this does not reflect the reality.

Proposals for pre- and post-assessments are mandated by many proposed policy frameworks that address algorithmic management, as well as Data Protection Impact Assessments (DPIAs).[224] We have outlined a set of concerns with auditing as a general practice in the Accountability section, and these considerations all apply in this context. While audits may have the positive effect of providing a basis for referring cases to governmental agencies that oversee workplace conditions and employment discrimination, such as the Department of Labor, the US Occupational Safety and Health Administration, and the US Equal Employment Opportunity Commission, these referrals could be made on other forms of evidence.

In particular, skewed incentives on the part of employers and software vendors raise real questions around whether auditors could ever gain meaningful access to the information needed to effectively conduct an audit.[225] Furthermore, the likelihood that a company would assert trade secrecy over the results of an audit is high, leading to questions around what information from an audit will be made public and who gets to decide. This has already been made plain in the example of the AI hiring company HireVue's attempt to selectively release results from an independent audit it commissioned in an attempt to prove its software is unbiased. It mischaracterized the breadth of the audit, excluding in particular the facial analysis and employee performance predictions HireVue had been criticized for.[226] This example illustrates how audits can be wielded by companies as a mechanism to feign an interest in accountability while evading more stringent accountability measures.

[221] Ben Green and Amba Kak, "The False Comfort of Human Oversight as an Antidote to A.I. Harm," *Slate*, June 15, 2021.
[222] Peter Fussey and Daragh Murray, "Policing Uses of Live Facial Recognition in the United Kingdom," AI Now Institute, September 2020.
[223] Austin Clyde, "Human-in-the-Loop Systems Are No Panacea for AI Accountability," Tech Policy Press, December 1, 2021; Niamh McIntyre, Rosie Bradbury, and Billy Perrigo, "Behind TikTok's Boom: A Legion of Traumatised, $10-a-Day Content Moderators," Bureau of Investigative Journalism, October 20, 2022; Adrienne Williams, Milagros Miceli, and Timnit Gebru, "The Exploited Labor Behind Artificial Intelligence," *Noema*, October 13, 2022.
[224] See Worker Rights: Workplace Technology Accountability Act, A.B. 1651; and European Commission, "Proposal for a Directive of the European Parliament and of the Council on Improving Working Conditions in Platform Work."
[225] See Ada Lovelace Institute and DataKind UK, "Examining the Black Box: Tools for Assessing Algorithmic Systems," April 2020; and Mathias Vermeulen, "The Keys to the Kingdom," Knight First Amendment Institute at Columbia University, July 27, 2021.
[226] Alex C. Engler, "Independent Auditors Are Struggling to Hold AI Companies Accountable," *Fast Company*, January 26, 2021.

Third, determining who has the requisite expertise to conduct an effective audit, particularly in the absence of any industry standards, remains an open question. (See also: Algorithmic Accountability) At the most fundamental level, auditing is premised on the idea that the use of these systems is meaningfully contestable, which is a poor reflection of the power dynamics between employers and workers.

### Data protection regulations offer inroads to enforcement today, but don't go far enough.

Recent regulatory efforts focused on data protection largely exempt workplaces, though amendments to the California Consumer Privacy Act took effect in January 2023 that extended its protections to workers at large firms.[227] Primarily based on the understanding that the consent frameworks central to most data protection policy break down in the context of work, workplace exceptions result in a major carveout under data protection law. In practice, this has meant that in the United States workers are being left out of the wave of interest in privacy regulation, even as surveillance of workplaces is undergoing significant expansion.

Conversely, a handful of regulations in the European context are being used very effectively by unions and worker collectives to sue for information on algorithmic management. For example, the App Drivers and Couriers Union has sued Uber under the EU General Data Protection Regulation (GDPR) to lay claim to rights over the data and algorithms used to determine rideshare drivers' pay.[228]

Researchers argue that existing EU data protection regulations already provide tools to enable a stronger enforcement posture toward the use of worker surveillance and algorithmic management.[229] Such proposals largely turn to the GDPR, EU AI Act, and CCPA to assert that many of the above policy measures are already accounted for in existing law. For example, the GDPR already requires notice to data subjects when they are involved in algorithmic decision-making and profiling, though it remains unclear whether firms using algorithmic management systems are doing so.[230] It is also likely that the GDPR's Article 35 requirements necessitating the use of a Data Protection Impact Assessment would apply to uses in the workplace context, and that a DPIA should be conducted both prior to deployment of an algorithmic decision-making system at work and iteratively thereafter.[231]

But even here, policy measures that originate from data protection laws largely fall into the trap outlined above in which the burden is placed on those harmed by these systems rather than those who benefit from them. Courts have reinforced these weaknesses by concluding that the GDPR is designed for transparency related to violations of the law, rather than to achieve broader objectives such as ensuring workers are generally informed of what information is collected about them.[232] A new generation of "data minimization" policy measures advocated for by civil society organizations and legislative proposals offer greater promise. These include stronger restrictions on the collection of

[227] Daniel Geer, Charles P. Pfleeger, Bruce Schneier, John S. Quarterman, Perry Metzger, Rebecca Bace, and Peter Gutmann, "CyberInsecurity: The Cost of Monopoly: How the Dominance of Microsoft's Products Poses a Risk to Security," Schneier on Security, September 24, 2003.
[228] See Dubal, "On Algorithmic Wage Discrimination," 10; and Natasha Lomas, "Ola Is Facing a Drivers' Legal Challenge over Data Access Rights and Algorithmic Management," TechCrunch, September 10, 2020.
[229] Antonio Aloisi, "Regulating Algorithmic Management at Work in the European Union: Data Protection, Non-Discrimination and Collective Rights," *International Journal of Comparative Labour Law and Industrial Relations*, forthcoming, accessed March 3, 2023.
[230] (GDPR Art 13(2)(f) and Art 14 (2)(g); see also Intersoft Consulting, "Art. 13 GDPR: Information to Be Provided Where Personal Data Are Collected from the Data Subject," n.d., accessed March 3, 2023; and Intersoft Consulting, "Art. 14 GDPR: Information to Be Provided Where Personal Data Have Not Been Obtained from the Data Subject," n.d., accessed March 3, 2023.
[231] Aloisi, "Regulating Algorithmic Management at Work in the European Union."
[232] Dubal, "On Algorithmic Wage Discrimination," 46.

specific types of data (eg. biometrics) or restrictions on use of such data in certain types of contexts (eg. workplaces, schools, hiring), but it remains unclear to what extent some of these would apply to the work or employment context. (See also: Data Minimization).

## Building Worker Power through Tech Policy

Given that worker surveillance protections would likely develop independently of more general privacy regulations in the United States, there is an opportunity to move away from the traditional data protection paradigm and to formulate worker surveillance laws that attend more effectively to information asymmetries, while retaining the provisions that make the most sense (purpose and collection limitations and rights to access data).

First, these measures could focus on what can be inferred about workers using algorithmic methods—their outcomes—rather than solely focusing on how data is collected and what happens to that data. This is particularly important given the shift toward first-party profiling activities by tech firms, reliance on anonymization, differential privacy and synthetic production of data, and increased ability to draw inferences using machine learning techniques without direct tracking of individual data at all. Such an approach could include the use of data that is anonymized but still used to harm workers as a collective. One example of this is the collection of workplace data that allows companies to try to predict which stores and locations are most likely to unionize and prepare or preemptively deploy union-busting techniques.[233]

Second, any future-looking rights framework should proceed from an impact-oriented definition of data that includes contexts of collective (rather than individualized) harm. Such an approach would more effectively provide protection against interference or oversight of protected concerted activity, bringing algorithmic management policy in line with baseline labor rights protections. Rather than focus on securing data as the object of analysis, policy proposals could adopt an approach that foregrounds how data and algorithmic models are instrumentalized as a mode of control and means of eroding autonomy and collective power: fundamentally, the issues at hand are not about data, but about the relationships and structural inequities between workers and employers.

[233] See Sarah Kessler, "Companies Are Using Employee Survey Data to Predict—and Squash—Union Organizing," OneZero, Medium, July 30, 2020; and Shirin Ghaffary and Jason Del Rey, "The Real Cost of Amazon," Vox, June 29, 2020.

Spotlight

# Tech and Financial Capital

Tech firms are wielding unprecedented amounts of capital to expand their base of power in creative ways. Civil society should explore structural points for intervention.

The financial picture for the tech industry as a whole looks bleaker than it has in the past decade, as the industry grapples with the consequences of rampant speculation: waves of layoffs,[234] the collapse of crypto markets,[235] and the failure of Silicon Valley Bank[236] are all indicators of further turmoil. These environmental shifts are likely to concentrate resources even more deeply within the biggest firms, which are less dependent on venture capital and leveraged debt, and thus will weather—and may even benefit from—the storm.

These firms hold an unprecedented amount of financial capital[237] and wield this capital using a variety of strategies to tilt the playing field in their favor and reduce risks to their bottom line. This makes tech capital strategies a critical site for tech accountability. Researchers and advocates are increasingly scrutinizing the ways in which tech firms are influencing the funding landscape for tech policy, but this could go further, accounting for the broad scope of tech industry capital strategies as structural points for intervention.

As Meredith Whittaker highlighted in research examining interdependencies between tech firms and the AI field, tech firms "are startlingly well-positioned to shape what we do—and do not—know about AI and the business around it, at the same time that their AI products are working to shape our lives and institutions. "[238] This is explicitly reinforced in a document leaked in 2020 that outlined Google's playbook for influencing the European Commission as regulators began work on the DMA and DSA: the company sought to leverage academic researchers to raise questions about the proposed rules, attempted to erode support through lobbying MEPs, and seeded a trade dispute across the Atlantic by

[234] Issie Lapowsky and Erin Wong, "Tech's Very Bad Year, in Numbers," Rest of World, March 13, 2023, https://restofworld.org/2023/techs-bad-year-global-layoffs-data.

[235] See Vicky Ge Huang, Alexander Osipovich, and Patricia Kowsmann, "FTX Tapped Into Customer Accounts to Fund Risky Bets, Setting Up Its Downfall," *Wall Street Journal*, November 11, 2022, https://www.wsj.com/articles/ftx-tapped-into-customer-accounts-to-fund-risky-bets-setting-up-its-downfall-11668093732; and David Yaffe-Bellany, "How Sam Bankman-Fried's Crypto Empire Collapsed," *New York Times*, November 14, 2022, https://www.nytimes.com/2022/11/14/technology/ftx-sam-bankman-fried-crypto-bankruptcy.html.

[236] Rachel Louise Ensign, Corrie Driebusch, and Meghan Bobrowsky, "Silicon Valley Bank Closed by Regulators, FDIC Takes Control," *Wall Street Journal*, March 10, 2023, https://www.wsj.com/articles/svb-financial-pulls-capital-raise-explores-alternatives-including-possible-sale-sources-say-11de7522.

[237] Alex Wilhelm, "Big Tech Is Now Worth So Much We've Forgotten to Be Shocked by the Numbers," TechCrunch, May 1, 2021, https://techcrunch.com/2021/05/01/big-tech-is-now-worth-so-much-weve-forgotten-to-be-shocked-by-the-numbers.

[238] Meredith Whittaker, "The Steep Cost of Capture," *Interactions* 28, no. 6 (November–December 2021): 51, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4135581.

encouraging US officials to take stances in opposition to the policy.[239] But the industry is not inventing the wheel here; for decades, corporate actors have utilized their capital to adopt a diverse set of nonmarket strategies designed to tilt the cards in their favor.[240]

These include:

1. **Lobbying:** firms can use their capital to directly lobby for policy changes.
    a. In the first half of 2020, Google, Facebook, Apple, and Microsoft spent $23 million combined for lobbying in the European Union. This is equal to the entirety of their lobbying spending in the year prior.[241] In the US, the companies behaved similarly, increasing their lobbying spending to $55 million in 2021, an increase from $34 million in 2020.[242]
    b. Big Tech firms have also funded 'industry coalitions'[243] such as the Chamber of Progress and lobbying groups like the Connected Commerce Council to purportedly represent the interests of small businesses in opposition to antitrust and other regulatory movements. Many of the small businesses listed on the membership roll of the Connected Commerce Council reported being unaware their names were being used.[244]
2. **Staffing and recruiting from government:** the "revolving door" is frequently employed by firms both to gain detailed insights into regulatory agencies and to seek to influence them.
    a. Nearly half—26 of 56—of the members of a European Commission high-level expert group on artificial intelligence represented business interests.[245]
    b. All 12 of the former national security leaders who warned antitrust enforcement would make the US less competitive with China were revealed to have ties with major tech companies.[246]
    c. The Defense Innovation Advisory Board (DIAB), designed to advise the Defense Department on how best to employ technology, was chaired by Former Google CEO Eric Schmidt, and counted among its members Amazon CEO Jeff Bezos, LinkedIn cofounder Reid Hoffman, and Instagram COO Marne Levine, alongside others.[247]

[239] Adam Satariano and Matina Stevis-Gridneff, "Big Tech Turns Its Lobbyists Loose on Europe, Alarming Regulators," *New York Times*, December 14, 2020, https://www.nytimes.com/2020/12/14/technology/big-tech-lobbying-europe.html.
[240] Zephyr Teachout and Lina Khan, "Market Structure and Political Law: A Taxonomy of Power," *Duke Journal of Constitutional Law & Public Policy* 9, no. 1 (2014): 37–74, https://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=1087&context=djclpp.
[241] Satariano and Stevis-Gridneff, "Big Tech Turns Its Lobbyists Loose on Europe."
[242] Emily Birnbaum, "Tech Spent Big on Lobbying Last Year," *Politico*, January 24, 2022, https://www.politico.com/newsletters/morning-tech/2022/01/24/tech-spent-big-on-lobbying-last-year-00001144.
[243] Chamber of Progress, https://progresschamber.org/
[244] Emily Birnbaum, "Group Backed By Tech Giants Claims Thousands of Members", *Politico,* March 30, 2022, https://www.politico.com/news/2022/03/30/connected-commerce-council-amazon-google-lobbying-00021801.
[245] Camille Schyns, Greta Rosén Fondahn, Alina Yanchur, and Sarah Pilz, "How Big Tech Dominates EU's AI Ethics Group," *EUobserver*, November 3, 2021, https://euobserver.com/investigations/153386.
[246] Emily Birnbaum, "12 Former Security Officials Who Warned against Antitrust Crackdown Have Tech Ties," *Politico*, September 22, 2021, https://www.politico.com/news/2021/09/22/former-security-officials-antitrust-tech-ties-513657.
[247] U.S. Department of Defense, "Secretary Carter Names Additional Members of Defense Innovation Advisory Board," press release, July 26, 2016, https://www.defense.gov/News/Releases/Release/Article/857710/secretary-carter-names-additional-members-of-defense-innovation-advisory-board.

d. Schmidt has lobbied for the passage of the 2023 National Defense Authorization Act, a bill to determine government defense spending that contains amendments referencing specific recommendations of the National Security Commission on Artificial Intelligence.[248] This bill would include appropriations for the new chief digital and artificial intelligence officer, Craig Martell, who has publicly stated that Schmidt picked him for the role.[249]

e. Under the tenure of former White House Chief Science Adviser Eric Lander, who served on the DIAB alongside Eric Schmidt, more than a dozen staff members of the Office of Science and Technology Policy had a relationship to Schmidt or were paid by him.[250] Schmidt Futures paid the salaries of two employees in the Office, and Schmidt Futures' chief innovation officer remained on the firm's payroll while working as an unpaid consultant for the White House.[251] The employee eventually left following ethics complaints, while the General Counsel's office raised "significant" ethical concerns around the salary arrangement.[252]

3. **Creating biased information:** firms leverage the credibility of academic research through funding to create the appearance of objective evidence to support their policy objectives.[253] Even without direct influence on the substance of the research (though they do sometimes assert this as well),[254] in the current precarious funding climate this can have a significant impact on which research agendas receive support.[255]

    a. Amazon funded a $20 million program on fairness in AI, leading to concerns that the program amounts to "ethics washing."[256] Researcher Yochai Benkler wrote in *Nature* that "when the NSF lends Amazon the legitimacy of its process for a $7.6-million programme (0.03% of Amazon's 2018 research and development spending), it undermines the role of public research as a counterweight to industry-funded research."[257]

[248] Eamon Javers, "How Google's Former CEO Eric Schmidt Helped Write A.I. Laws in Washington without Publicly Disclosing Investments in A.I. Startups," CNBC, October 24, 2022, https://www.cnbc.com/2022/10/24/how-googles-former-ceo-eric-schmidt-helped-write-ai-laws-in-washington-without-publicly-disclosing-investments-in-ai-start-ups.html.

[249] Kate Kaye, "Inside Eric Schmidt's push to profit from an AI cold war with China," *Protocol*, October 31, 2022, https://www.protocol.com/enterprise/eric-schmidt-ai-china.

[250] Alex Thompson, "A Google Billionaire's Fingerprints Are All over Biden's Science Office," *Politico*, March 28, 2022, https://www.politico.com/news/2022/03/28/google-billionaire-joe-biden-science-office-00020712.

[251] Ibid.

[252] Ibid. Lander eventually resigned following an investigation that concluded he violated White House workplace policy by bullying and demeaning OSTP staff. See Alex Thompson, "Biden's Top Science Adviser Bullied and Demeaned Subordinates, According to White House Investigation," *Politico*, February 7, 2022, https://www.politico.com/news/2022/02/07/eric-lander-white-house-investigation-00006077.

[253] See Mohamed Abdalla and Moustafa Abdalla, "The Grey Hoodie Project: Big Tobacco, Big Tech, and the Threat on Academic Integrity," arXiv:2009.13676v4, April 27, 2021, https://arxiv.org/pdf/2009.13676.pdf; and "Gig Economy Project – Uber whistleblower Mark MacGann's full statement to the European Parliament," Brave New Europe, October 25, 2022, https://braveneweurope.com/uber-whistleblower-mark-macganns-full-statement-to-the-european-parliament.

[254] Most notoriously, Uber exerted influence over the calculations used by Cornell economists in a study that concluded 92 percent of drivers made above minimum wage. A study using similar data conducted independently found that the majority of drivers earned far less. Both studies were conducted and published shortly before legislative battles in California and Washington state to determine the employment status of rideshare drivers. See Veena Dubal, "On Algorithmic Wage Discrimination," January 19, 2023, http://dx.doi.org/10.2139/ssrn.4331080, 12–14; and Hubert Horan, "Uber's "Academic Research" Program: How to Use Famous Economists to Spread Corporate Narratives," *ProMarket*, December 5, 2019, https://www.promarket.org/2019/12/05/ubers-academic-research-program-how-to-use-famous-economists-to-spread-corporate-narratives.

[255] Whittaker, "The Steep Cost of Capture."

[256] Benjamin Romano, "Amazon's Role in Co-Sponsoring Research on Fairness in AI Draws Mixed Reaction," *Seattle Times*, March 31, 2019, https://www.seattletimes.com/business/amazon/amazons-role-in-co-sponsoring-research-on-fairness-in-a-i-draws-mixed-reaction.

[257] Yochai Benkler, "Don't Let Industry Write the Rules for AI," *Nature*, May 1, 2019, https://www.nature.com/articles/d41586-019-01413-1.

   b. Google, Amazon, and Qualcomm are among the largest donors to the Global Antitrust Institute at George Mason University, focused on fostering a hands-off approach to antitrust law.[258]

4. **Directing the politics of employees and contractors:** companies are able to direct their employees expressly or implicitly to adopt certain political stances.

   a. One of the starkest ways the tech industry has done this is through retaliation against its most outspoken employees. For example, Amazon fired two employees engaged in environmental organizing,[259] and Google let go members of its Ethical AI team after they raised concerns about potential harms from the company's development of large language models.[260]

5. **Power derived from being "too big to fail":** as tech firms increasingly take on the functions of critical infrastructure, this may lead to increased reticence to regulate in a manner that could lead to system failure.

   a. Financial regulators have expressed concerns that increased dependency of financial systems, including payment systems, on cloud firms poses risks to financial stability and could render these companies too big to fail.[261]

   b. Tech firms receive financial benefits due to their unique economic position, receive lower bond funding costs, and are treated as a "stable asset" during moments of market turbulence.[262]

Collectively, these examples illustrate the multifaceted ways in which tech firms wield their capital to assert their influence over and above more traditional policy advocacy. Some of these strategies and tactics can also be used in the effort to achieve tech accountability. For example, labor unions have historically leveraged their holdings in public pension funds as a lever for shareholder advocacy in order to seek changes in corporations, such as narrowing the gap between worker and executive compensation.[263]

In a number of cases, shareholder proposals have been used to make efforts toward advocating for greater diversity and inclusion measures at the leadership level of companies; for stronger lobbying disclosures; and for mandating evaluations of companies' impact on human rights. These efforts have met with varying degrees of success.

[258] Daisuke Wakabayashi, "Big Tech Funds a Think Tank Pushing for Fewer Rules. For Big Tech," *New York Times*, July 24, 2020, https://www.nytimes.com/2020/07/24/technology/global-antitrust-institute-google-amazon-qualcomm.html.

[259] "Amazon 'Illegally Retaliated' against Climate Activists," BBC News, April 5, 2021, https://www.bbc.co.uk/news/business-56641847.

[260] Cade Metz and Daisuke Wakabayashi, "Google Researcher Says She Was Fired over Paper Highlighting Bias in A.I.," *New York Times*, December 3, 2020, https://www.nytimes.com/2020/12/03/technology/google-researcher-timnit-gebru.html.

[261] Iain Withers and Huw Jones, "For Bank Regulators, Tech Giants Are Now Too Big to Fail," Reuters, August 20, 2021, https://www.reuters.com/world/the-great-reboot/bank-regulators-tech-giants-are-now-too-big-fail-2021-08-20.

[262] Nordine Abidi and Ixart Miquel-Flores, "Too Tech to Fail?" Faculty of Law Blogs, University of Oxford, July 13, 2022, https://blogs.law.ox.ac.uk/business-law-blog/blog/2022/07/too-tech-fail.

[263] See Sanford M. Jacoby, *Labor in the Age of Finance: Pensions, Politics, and Corporations from Deindustrialization to Dodd-Frank* (Princeton: Princeton University Press, 2021); Justice for Janitors, 2022, accessed March 15, 2023, https://www.justiceforjanitors.org; and Christian Wihtol, "Providence, SEIU Clash Over High Exec Pay, Union Push," Lund Report, January 12, 2019, https://www.thelundreport.org/content/providence-seiu-clash-over-high-exec-pay-union-push.

- In 2022, Amazon agreed to conduct a racial equity audit, to be led by former US Attorney General Loretta Lynch, in response to a shareholder proposal filed by New York State Comptroller Thomas DiNapoli for an independent racial equity audit.[264]

- In May 2022, Amazon warehouse picked Daniel Olayiwola introduced a proposal at Amazon's annual shareholder meeting calling for the company to end its 'injury crisis' by eliminating productivity quotas and mechanisms that lead workers to prioritize speed over safety or else lose their jobs. The measure was voted down at the company's annual meeting.[265]

- In 2021, Microsoft agreed to commission an independent third-party assessment to "identify, understand, assess, and address actual or potential adverse human rights impacts" after shareholders filed a proposal asking the board to evaluate how effectively the company implements its Human Rights Statement, including review of Microsoft's contracts with US Immigration and Customs Enforcement and Customs and Border protection. The shareholders withdrew the proposal after Microsoft's announcement.[266]

- Subsequent proposals filed the same year by Harrington Investments and the Sisters of St. Joseph of Peace, a congregation of nuns, demanded that Microsoft prohibit the sale of facial recognition technology to all government entities, called for a more holistic report on Microsoft's human rights practices, and asked Microsoft to commission a report on how its lobbying aligns with its stated principles.[267] The latter proposal was withdrawn following a commitment from Microsoft to improve its disclosures on lobbying engagement and an affirmation of how its efforts align with the company's stated social and environmental values.[268]

- Google employee Irene Knapp went before a Google shareholder meeting in 2018 to present a proposal, ultimately voted down, on behalf of Zevin Asset Management that would have required that Alphabet's executive compensation be tied to gender, racial, and ethnic diversity metrics in employee recruiting and retention.[269]

- Apple shareholders have approved proposals requiring the company to conduct a third-party civil rights audit, against Apple's recommendation.[270]

[264] See Annie Palmer, "Amazon to Conduct Racial-Equity Audit Led by Former Attorney General Loretta Lynch," CNBC, April 18, 2022, https://www.cnbc.com/2022/04/18/amazon-to-conduct-racial-equity-audit-led-by-former-ag-loretta-lynch.html; and Office of the New York State Comptroller, NYS Comptroller Thomas P. DiNapoli, "Racial Equity Audit," 2022, accessed March 15, 2023, https://www.osc.state.ny.us/files/press/pdf/nycrf-amazon-shareholder-proposal.pdf.

[265] See Albert Samaha, "Amazon Warehouse Worker Daniel Olayiwola Decided To Make A Podcast About Amazon's Working Conditions", *BuzzFeed News*, February 16, 2023, https://www.buzzfeednews.com/article/albertsamaha/daniel-olayiwola-amazon-scamazon-podcast, Caitlin Harrington, "An Amazon Warehouse Worker Takes the Fight to Shareholders," *Wired*, May 25, 2022, https://www.wired.com/story/amazon-warehouse-worker-shareholder-proposal; Sebastian Klovig Skelton, "Amazon Shareholders Vote Down Audit of Warehouse Work Conditions," *Computer Weekly*, May 27, 2022, https://www.computerweekly.com/news/252520759/Amazon-shareholders-vote-down-audit-of-warehouse-work-conditions.

[266] Open MIC, "Facing Investor Pressure, Microsoft Agrees to Publish Independent Human Rights Impact Assessment, Including Review of Surveillance and Law Enforcement Contracts," press release, October 31, 2021, https://www.openmic.org/news/2021/facing-investor-pressure-microsoft-agrees-to-publish-independent-human-rights-impact-assessment-including-review-of-surveillance-and-law-enforcement-contracts.

[267] See Chris Mills Rodrigo, "Exclusive: Scrutiny Mounts on Microsoft's Surveillance Technology," *Hill*, June 17, 2021, https://thehill.com/policy/technology/558890-exclusive-scrutiny-mounts-on-microsofts-surveillance-technology; and Issie Lapowsky, "These Nuns Could Force Microsoft to Put Its Money Where Its Mouth Is," *Protocol*, November 19, 2021, https://www.protocol.com/policy/microsoft-lobbying-shareholder-proposal.

[268] "Microsoft Pledges to Improve Lobbying Disclosures in Agreement with Investors," Investor Advocates for Social Justice, November 16, 2022, https://iasj.org/microsoft-pledges-to-improve-lobbying-disclosures-in-agreement-with-investors.

[269] See Jillian D'Onfro, "Here's the Statement a Google Employee Read Today Criticizing the Company's Diversity Efforts," CNBC, June 6, 2018, https://www.cnbc.com/2018/06/06/google-engineer-reads-shareholder-proposal.html; and Zevin Asset Management, LLC, "Alphabet Inc. (GOOGL) Shareholder Proposal Number 8: Integrating Sustainability & Diversity Metrics into Executive Compensation," 2018, https://www.sec.gov/Archives/edgar/data/1394096/000121465918003664/b514180px14a6g.htm.

[270] See Kif Leswing, "Shareholders Vote for Apple to Conduct a Civil Rights Audit, Bucking Company's Recommendation," CNBC, March 4, 2022, https://www.cnbc.com/2022/03/04/apple-shareholders-vote-for-company-to-conduct-a-civil-rights-audit.html; and United States Securities and

As tech firms undergo rounds of layoffs, ostensibly because of financial headwinds, these capital strategies deserve to be scrutinized all the more closely. In doing so, accountability advocates can attend to the shifting playbook used by companies to influence potential regulation and explore possible inroads that can still be used to advocate for change.

Exchange Commission, Form 8-K, Current Report Pursuant to Section 13 OR 15(d) of the Securities Exchange Act of 1934, March 4, 2022, https://www.sec.gov/ix?doc=/Archives/edgar/data/320193/000119312522066169/d294699d8k.htm.

Antitrust and Competition

# It’s Time for Structural Reforms to Big Tech

Competition policy is poised to become a core part of the tech accountability tool kit. We’ll need it to curb the antidemocratic effects of concentrated tech power.

**Weak enforcement of antitrust laws by government has allowed a handful of Big Tech companies to mediate many domains of life. But a reinvigorated interest in antitrust enforcement is cutting to the heart of concentrated tech power.**

Over the past two decades, a handful of tech firms have adopted policies and infrastructural designs that enabled them to grow their power massively.[271] They were enabled by conservative and hands-off enforcement of antitrust laws, in combination with an “innovation”-centered US tech policy agenda that treated tech companies like national champions.[272] These firms intentionally took an approach that would ensure their eventual dominance: they rapidly and aggressively acquired competitors as they emerged,[273] leveraging data they were able to vacuum up through surveillance and acquisition to favor their own products and reinforce their dominance.[274] They specifically designed their systems with the intent to lock in users, raising the costs to switch to different platforms.[275] They built marketplaces in

[271] See Lina M. Khan, “Sources of Tech Platform Power,” *Georgetown Law Technology Review* 2, no.2, (2018): 325–334, https://georgetownlawtechreview.org/wp-content/uploads/2018/07/2.2-Khan-pp-225-34.pdf; and K. Sabeel Rahman, “The New Utilities: Private Power, Social Infrastructure, and the Revival of the Public Utility Concept,” *Cardozo Law Review* 39, no. 5 (2018): 1621–1689, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2986387.

[272] Daniel Schiller, *Digital Capitalism: Networking the Global Market System* (Cambridge, MA: MIT Press, 2000).

[273] See Tim Wu and Stuart A. Thompson, “The Roots of Big Tech Run Disturbingly Deep,” *New York Times*, June 7, 2019, https://www.nytimes.com/interactive/2019/06/07/opinion/google-facebook-mergers-acquisitions-antitrust.html; and DensityDesign Lab and Tactical Tech, GAFAM Empire, 2022, accessed March 3, 2023, https://gafam.theglassroom.org.

[274] See for example Steve Lohr, “This Deal Helped Turn Google into an Ad Powerhouse. Is That a Problem?” *New York Times*, September 21, 2020, https://www.nytimes.com/2020/09/21/technology/google-doubleclick-antitrust-ads.html; and Khari Johnson, “The iRobot Deal Would Give Amazon Maps inside Millions of Homes,” *Wired*, August 5, 2022, https://www.wired.com/story/amazon-irobot-roomba-acquisition-data-privacy.

[275] See OECD, “Data Portability, Interoperability and Digital Platform Competition,” OECD Competition Committee Discussion Paper, 2021, https://www.oecd.org/daf/competition/data-portability-interoperability-and-digital-platform-competition-2021.pdf; and Investigation of Competition in Digital Markets, CP 117–8, Part 1, 117th Congress, July 2022, https://www.govinfo.gov/content/pkg/CPRT-117HPRT47832/pdf/CPRT-117HPRT47832.pdf.

which they themselves competed, boosting their own products over those of third party competitors.[276] Without regulatory friction[277] or even much public oversight, they built an ecosystem in which it is now virtually impossible to escape the technological systems of a handful of firms.[278] None of this is the byproduct of innovation; it's just a markedly aggressive business strategy that was amply financed by the venture capital sector without requiring firms turn a profit or even meaningfully contribute to the public good.

But at long last, policymakers are poised for change. An emerging policy perspective aims to aggressively curb these practices and introduce a stronger set of checks and balances on tech corporate power.[279] This upswell is occurring within enforcement agencies in countries around the globe, through the appointments of Lina Khan, Jonathan Kanter and Tim Wu to leadership positions in the US government and with policy movements taking place in the US[280] and EU,[281] Australia,[282] South Korea,[283] and India,[284] among others.

Competition law is well designed for this purpose. It provides for both structural and behavioral remedies that can, when combined, end the kinds of practices that have allowed these companies to get so big.[285] It includes both *ex ante* interventions that can prevent firms from gaining too much market power and *ex post* enforcement measures that can address abuses of dominance when they occur.

This revitalized perspective on the proper role of competition law hearkens back to the origins of trust-busting (an era during which Progressives sought to break up monopolies and their hold on American industry and politics), and its recognition of the antidemocratic effects of consolidated economic power.[286] This reinvigoration of antitrust doctrine marks a long overdue return to the original goals of the law: since the 1980s, antitrust enforcers have largely taken the view that corporate consolidation isn't necessarily harmful if it doesn't lead to higher prices, a legal doctrine referred to as

[276] See European Commission, "Antitrust: Commission Sends Statement of Objections to Amazon for the Use of Non-Public Independent Seller Data and Opens Second Investigation into its E-commerce Business Practices," press release, November 10, 2020, https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2077; and European Commission, Information on the Commission's Initiation of Antitrust Proceedings in Case AT.40703, November 10, 2020, https://ec.europa.eu/competition/antitrust/cases/dec_docs/40703/40703_67_4.pdf.

[277] Paul Ohm and Brett Frischmann, "Governance Seams," Iowa Innovation, Business & Law Center, Iowa College of Law, n.d., accessed March 3, 2023, https://ibl.law.uiowa.edu/governance-seams.

[278] Kashmir Hill, "I Tried to Live without the Tech Giants. It Was Impossible," *New York Times*, July 31, 2020, https://www.nytimes.com/2020/07/31/technology/blocking-the-tech-giants.html.

[279] Ibid. See also Lina M. Khan, "The Ideological Roots of America's Market Power Problem," *Yale Law Journal Forum*, June 4, 2018, https://www.yalelawjournal.org/forum/the-ideological-roots-of-americas-market-power-problem; Sandeep Vaheesan, "The Twilight of the Technocrats' Monopoly on Antitrust?" *Yale Law Journal Forum*, June 4, 2018, https://www.yalelawjournal.org/forum/the-twilight-of-the-technocrats-monopoly-on-antitrust; and Tim Wu, *The Curse of Bigness: Antitrust in the New Gilded Age* (New York: Columbia Global Reports, 2018).

[280] Investigation of Competition in Digital Markets, CP 117–8, Part 1, 117th Congress, July 2022, https://www.govinfo.gov/content/pkg/CPRT-117HPRT47832/pdf/CPRT-117HPRT47832.pdf.

[281] European Commission, "Digital Markets Act: Rules for Digital Gatekeepers to Ensure Open Markets Enter into Force," press release, October 31, 2022, https://ec.europa.eu/commission/presscorner/detail/en/ip_22_6423.

[282] Australian Competition & Consumer Commission, "Digital Platform Services Inquiry 2020–25: Project Overview," n.d., accessed March 3, 2023, https://www.accc.gov.au/focus-areas/inquiries-ongoing/digital-platform-services-inquiry-2020-25.

[283] "South Korea Approves Rules on App Store Law Targeting Apple, Google," Reuters, March 8, 2022, https://www.reuters.com/technology/skorea-approves-rules-app-store-law-targeting-apple-google-2022-03-08.

[284] Sourabh Jain, "India's Competition Watchdog Is Probing Deals between Amazon, Flipkart and Their Preferred Sellers," *Business Insider India*, May 31, 2022, https://www.businessinsider.in/business/ecommerce/news/indias-competition-watchdog-is-probing-deals-between-amazon-flipkart-and-their-preferred-sellers/articleshow/91909512.cms.

[285] Lina M. Khan, "The Separation of Platforms and Commerce," Columbia Law Review 119, no. 4 (May 2019): 973–1098, https://columbialawreview.org/content/the-separation-of-platforms-and-commerce.

[286] "Sherman Anti-Trust Act (1890)," Milestone Documents, National Archives, accessed March 3, 2023, https://www.archives.gov/milestone-documents/sherman-anti-trust-act.

the *consumer welfare standard.*[287] This is a poor fit for addressing digital markets where consumers pay nothing to use services but nevertheless experience the harms of toxic competition.[288]

But it's going to take time, effort and—most importantly—resources in order to effect meaningful change in the power concentrated in tech firms. There are decades of legal precedent under the consumer welfare standard to contend with, and antitrust enforcers likely have tough battles ahead while they attempt to steer the ship back toward a more direct confrontation of the sources of corporate power. As DOJ antitrust head Jonathan Kanter put it: "Unless we give courts the opportunity to confront new fact patterns, new issues, new economic realities that are becoming pervasive throughout the economy, we're never really going to have the opportunity to advance the law in a way that makes it relevant and applicable to market realities and a modern economy."[289]

Even as they adopt a more muscular stance toward prosecuting Big Tech firms for antitrust violations in the courts, enforcement agencies are using other levers to make changes in the here and now: for example, the FTC and DOJ are pursuing a significant revision of the merger guidelines used to evaluate whether acquisitions by firms are anticompetitive.[290] The FTC updated its interpretation of Section 5 of the FTC Act, which addresses "unfair methods of competition," restoring legal authorities the FTC was charged to use by Congress but which the Commission largely left dormant in recent years.[291] And it is pursuing rulemakings, such as one recently proposed to prohibit the use of non-compete clauses that serve to prevent workers from switching jobs within the same industry on the basis that these employer agreements depress wages and are an unfair method of competition.[292]

The changes afoot will necessarily be slow, and will likely involve political losses: antitrust cases take years to move through the courts, and take significant investments of resources and time from the agencies that pursue them.[293] But these changes will be well worth the fight.

[287] Robert Bork, *The Antitrust Paradox: A Policy at War with Itself* (New York: Free Press, 1993).

[288] See Lina M. Khan, "Amazon's Antitrust Paradox," *Yale Law Journal* 126, no. 3 (January 2017): 710–787, https://www.yalelawjournal.org/pdf/e.710.Khan.805_zuvfyyeh.pdf; John M. Newman, "Antitrust in Zero-Price Markets: Foundations," *University of Pennsylvania Law Review* 164, no. 1 (December 2015): 149–206, https://www.pennlawreview.com/wp-content/uploads/2020/04/164-U-Pa-L-Rev-143.pdf; John M. Newman, Antitrust in Zero-Price Markets: Applications, *Washington University Law Review* 94, no. 1 (2016): 49–111, https://www.pennlawreview.com/wp-content/uploads/2020/04/164-U-Pa-L-Rev-143.pdf ; John M. Newman, Antitrust in Attention Markets: Objections and Responses, *Santa Clara Law Review* 59, no. 3 (2020): 743–769, https://repository.law.miami.edu/fac_articles/931; John M. Newman, "Antitrust in Digital Markets," *Vanderbilt Law Review* 72, no. 5 (2019): 1497–1561, https://repository.law.miami.edu/fac_articles/932; and Maurice E. Stucke, "The Relationship between Privacy and Antitrust," Notre Dame Law Review Reflection 97, no. 5 (2022): 400–417, https://ndlawreview.org/wp-content/uploads/2022/07/Stucke_97-Notre-Dame-L.-Rev.-Reflection-400-C.pdf.

[289] See Brian Fung, "The US Government Is Still Trying to Find Ways to Regulate Big Tech. He Has Some Ideas," CNN, January 11, 2023, https://www.cnn.com/2023/01/11/tech/jonathan-kanter-doj/index.html; see also Charlotte Slaiman, "No Pain, No Gain: FTC Loses Bid to Block Facebook's Acquisition of Within," Public Knowledge February 9, 2023, https://publicknowledge.org/no-pain-no-gain-ftc-loses-bid-to-block-facebooks-acquisition-of-within.

[290] Federal Trade Commission, "Federal Trade Commission and Justice Department Seek to Strengthen Enforcement Against Illegal Mergers," press release, January 18, 2022, https://www.ftc.gov/news-events/news/press-releases/2022/01/federal-trade-commission-justice-department-seek-strengthen-enforcement-against-illegal-mergers.

[291] Federal Trade Commission, "Policy Statement Regarding the Scope of Unfair Methods of Competition Under Section 5 of the Federal Trade Commission Act, Commission File No. P221202," November 10, 2022, https://www.ftc.gov/system/files/ftc_gov/pdf/P221202Section5PolicyStatement.pdf.

[292] Federal Trade Commission, "FTC Proposes Rule to Ban Noncompete Clauses, Which Hurt Workers and Harm Competition," press release, January 5, 2023, https://www.ftc.gov/news-events/news/press-releases/2023/01/ftc-proposes-rule-ban-noncompete-clauses-which-hurt-workers-harm-competition.

[293] See Kari Paul, "Google is facing the biggest antitrust case in a generation. What could happen?" *Guardian*, October 21, 2020, https://www.theguardian.com/technology/2020/oct/21/google-antitrust-charges-what-is-next; and Lauren Feiner, "The DOJ's Antitrust Case against Google Is Ambitious but Risky," CNBC, January 27, 2023, https://www.cnbc.com/2023/01/27/dojs-antitrust-case-against-google-is-ambitious-but-risky.html.

## Key Recent Transatlantic Antitrust Cases

**US Department of Justice vs. Google:**

The DOJ's case against Google is focused on Google's monopolization of the market in digital advertising. It describes how Google attained holdings across multiple parts of the digital advertising market, giving it monopoly power across publishers, ad impressions, and targeting data. It also portrays how, even with its dominant hold over the industry, Google used anticompetitive measures to head off potential future competitors. The DOJ is requesting several remedies in the case, including the divestiture of Google's Ad Manager suite and its ad exchange, AdX. The DOJ is also enjoining Google from continuing to engage in anticompetitive practices.

**European Commission vs. Amazon:**

The European Commission (EC) opened an investigation into Amazon's use of nonpublic data from its marketplace sellers, seeking to determine its impact on competition in digital marketplaces. It found that Amazon's use of nonpublic data distorted fair competition on its platform. It also opened a second, parallel investigation into whether Amazon was giving itself preferential treatment in the criteria it uses to determine who wins the Buy Box and in its program enabling sellers to offer products under Amazon Prime. The EC found that Amazon's rules and criteria unduly favored its own retail business and sellers that use Amazon's logistics and delivery services, and that the company abused its dominance in the French, German, and Spanish markets for the provision of online marketplace services to third party sellers. The EC and Amazon agreed to a set of commitments including treating sellers equally when determining the Buy Box winner, showing a second competing offer in the Buy Box, enabling independent carriers to directly contact Amazon customers, and allowing Prime sellers to freely choose any carrier for logistics and delivery services, among others. These commitments will remain in force for a duration of 5–7 years.

## Antitrust and/as Industrial Policy

**The US must abandon a narrow "national champions" approach that would disincentivize regulating Big Tech: instead, government must enact bold antitrust intervention that will create a more competitive ecosystem for all.**

Industrial policy, or the deliberate strategic effort by governments to encourage the development of particular sectors of the economy, offers a useful macro-level lens through which to view recent movements in antitrust and the path ahead. The European Union has been early and aggressive in its prosecution of Big Tech firms,[294] but arguably doing so also aligns with its economic interest: Europe's national champions have largely been eclipsed by US and Asian tech companies, and restoring competition in the tech industry is very much a strategic priority.[295] By contrast, US industrial policy in recent decades has largely focused on the expansion of US corporate dominance globally, and this has enabled US-based tech monopolies to reach the scope and scale that they have: their interests have broadly been interpreted as being in the US national interest.[296]

Historically, however, the United States has also acknowledged that allowing the concentration of unfettered monopoly power can create downstream political and governance harms, particularly where it begins to rival the power of the state—and this is reflected in the White House Executive Order on Promoting Competition in the American Economy, which acknowledges that America's growth and economic standing in the world is threatened by the problem of economic consolidation.[297] As the Order puts it, "the answer to the rising power of foreign monopolies and cartels is not the tolerance of domestic monopolization, but rather the promotion of competition and innovation by firms small and large, at home and worldwide."[298] And Tim Wu, a former adviser to the White House on technology and competition policy, recently argued that sound industrial policy makes its investments in support of foundational technology and ecosystems, rather than funding companies as national champions.[299]

As such, though it may be more challenging to overcome past precedent and the significant lobbying resources of Big Tech firms, both in terms of its doctrine and enforcement powers the United States is potentially much better positioned to enact the kinds of clear structural reforms that would lead to long-lasting change if it can move beyond stating its intentions toward making concerted interventions.

[294] See Javier Espinoza, "How Big Tech Lost the Antitrust Battle with Europe," *Financial Times*, March 21, 2022, https://www.ft.com/content/cbb1fe40-860d-4013-bfcf-b75ee6e30206; Samuel Stolton, "EU braces for Big Tech's legal backlash against new digital rulebook," *Politico*, August 10, 2022, https://www.politico.eu/article/eu-brace-legal-assault-against-digital-clampdown; and Steve Lohr, "To Rein In Big Tech, Europe Looked Beyond Lawsuits. Will the U.S. Follow?" *New York Times*, https://www.nytimes.com/2022/12/10/business/big-tech-antitrust-rules.html.

[295] "Emerging Non-European Monopolies in the Global AI Market," Future of Life Institute, November 2022, https://futureoflife.org/wp-content/uploads/2022/11/Emerging_Non-European_Monopolies_in_the_Global_AI_Market.pdf.

[296] Maurice E. Stucke and Ariel Ezrachi, "The Rise, Fall, and Rebirth of the U.S. Antitrust Movement," *Harvard Business Review*, December 15, 2017, https://hbr.org/2017/12/the-rise-fall-and-rebirth-of-the-u-s-antitrust-movement.

[297] White House, "Executive Order on Promoting Competition in the American Economy."

[298] Ibid.

[299] "The Internet's Midlife Crisis, Day 2 Keynote, Tim Wu," Silicon Flatirons, February 9, 2023, video, 44:35, https://youtu.be/89UfDmgL.

### Antitrust enforcement will be most effective where it engages how concentration in digital markets leads to—and results from—other kinds of tech-enabled harms.

A primary source of tech firms' power is their ability to leverage the unique insights derived from their platforms, insights that gain greater weight through their network effects.[300] Given the high level of concentration in the industry, these firms also use a variety of measures expressly designed to lock users into their ecosystem, making it harder to use other services and harder for new entrants to compete in a market.

Given this state of affairs, antitrust enforcement would be missing half the picture without also addressing how privacy, data protection, security, and other tech policy issues feed and are likewise shaped by the lack of competition in the tech industry. While enforcement agencies already have a number of tools at hand, many of the policy initiatives outlined below are designed with exactly this in mind. To boost their ability to pursue the unique nature of competition in digital markets, these proposals coalesce around a set of data-related issues that interface with competition specific to tech:

- **Data advantages:** Tech firms often try to acquire other firms to seek the additional insights that can be derived from their data. Some policy proposals seek to curb these data advantages by prohibiting firms from combining certain types of data streams, such as combining data collected from a covered platform and third-party data, or data across different lines of business, including recently acquired firms. Still others require that a firm can't condition the quality of service on a platform to a user consenting to give over their data. In other words, opting out of data collection can't result in a degradation of service.
- **Interoperability and data portability:** These provisions are designed to prohibit tech firms from building moats around their platforms, preventing (both consumer and business) users from switching to other services or leveraging insights from covered platforms.
- **Self-preferencing:** Many large tech firms operate marketplaces and also sell their own products on them. Several policy proposals mandate that these firms can't tip the scales by promoting their own offerings above others, such as in search rankings or in ad placement.[301]

[300] See Khan, "The Separation of Platforms and Commerce; and Khan, "Sources of Tech Platform Power."

[301] For example, a recent NBER study found that Amazon consistently ranks its own branded products higher than observably similar products in consumer search results. See Chiara Farronato, Andrey Fradkin and Alexander MacKay, "Self-Preferencing at Amazon: Evidence from Search Rankings," National Bureau of Economic Research (NBER), working paper 30894, January 2023, https://www.nber.org/papers/w30894.

# Antitrust Bills in Consideration

| Bill | Summary | |
|---|---|---|
| **HR 3826: Platform Competition and Opportunity Act of 2021** | Gives stronger tools to enforcement agencies to stop dominant platforms from acquiring direct and potential competitors, firms that reinforce or expand their market position, and data that strengthen or expand the platform's dominance. This bill shifts the burden in merger enforcement to the platform to demonstrate the merger isn't anticompetitive. | Go to bill > |
| **HR 3460: State Antitrust Enforcement Venue Act of 2022 (PASSED)** | Aims to promote competition by preventing the transfer of actions arising under the antitrust laws in which a State is a complainant. Prior to this bill, federal antitrust claims brought by states could be consolidated into federal multidistrict litigation (MDL) proceedings.<br>Reed Smith, "Defending against states' federal antitrust claims: Could a potential change to federal law make things a lot more complicated?" | Go to bill > |
| **HR 3843: Merger Filing Fee Modernization Act of 2022 (PASSED)** | Promotes antitrust enforcement by modifying and expanding the schedule for graduated merger filing fees and requiring that such fees be adjusted each year based on the Consumer Price Index. | Go to bill > |
| **HR 3849: ACCESS Act of 2021 or Augmenting Compatibility and Competition by Enabling Service Switching Act of 2021** | This bill requires large online platforms to facilitate consumers and businesses switching from one platform to another by allowing users to securely transfer user data to other platforms (portability) and allowing other platforms to connect and communicate with their systems (interoperability). | Go to bill > |
| **HR 3816: American Choice and Innovation Online Act** | Aims to prevent discriminatory conduct by forbidding a covered platform from a) undermining interoperability b) conditioning access to the covered platform on the purchase of other products/services owned by the covered platform c) using non-public data from a business user to offer/support the offering of the covered platform operator's own products/services d) restricting or impeding a business user from accessing data generated on the platform by the activities of the business user e) treating the covered platform operator's own products, services, or lines of business more favorably than those of another business user and f) interfering with a business user's pricing of goods/services. | Go to bill > |
| **HR 3825: Ending Platform Monopolies Act** | Aims to eliminate conflicts of interest by preventing covered platforms from owning or controlling a line of business other than the covered platform that a) utilizes the covered platform for the sale or provision of products or services b) offers a product or service that the covered platform requires a business user to purchase or utilize as a condition for access to the covered platform c) is a conflict of interest. It also includes prohibitions on conflicting board memberships. | Go to bill > |

### The European Union's Digital Markets Act will have important downstream implications for tech accountability, but will be part of a broader chorus of policy changes rather than its horizon.

The passage of the EU's Digital Markets Act adds a number of tools to regulators' tool kits to enable them to respond quickly to changes in the digital marketplace: from limits on combining data streams to transparency mandates.[302] Whether they will do so—and to what extent the DMA's guidelines will be self-enforceable—remains to be seen.[303]

The DMA will be applied adjacent to existing EU competition law, rather than as a replacement of existing statutes, and fills in a number of gaps in the current regulatory regime.[304] The DMA also will complement the GDPR, strengthening and extending some of its rules for user consent and enhancing data portability and transparency requirements for consumer profiling algorithms through a set of *ex ante* obligations. Distinct from the GDPR, the DMA is much more focused on business users than it is on individuals. It is designed with several goals in mind: to ensure that digital markets stay open to new entrants, to ensure fairness in the relationships between digital gatekeepers and business users, and to strengthen the internal market within the EU by harmonizing national regimes as they apply across the EU.

Several aspects of the DMA could strengthen tech accountability:

- **Restrictions on combining data silos:** The DMA limits the ability of Big Tech ("gatekeeper" firms) to combine multiple sources of data from disparate data streams in order to gain insights across their many platforms and business holdings. This would prevent firms from combining data across their holdings—for example, between Amazon Web Services and Amazon Marketplace—and those of third parties.

- **Restrictions on coercive "conditional consent":** This requires "gatekeeper" firms to offer less personalized but equivalent versions of the same platform to all users, regardless of whether the end user consents to give companies access to their data.[305]

- **Marketplace mandates:** Under the DMA, "gatekeeper firms" must allow their business users to curate their offerings across different kinds of marketplaces—for example, app makers should be able to tailor their offerings across Apple's App Store and Google's Android—and gatekeepers cannot bundle several platform services or combine them with identification services. This provision is designed to inhibit existing practices that lock business users into certain marketplaces and prevent them from offering different prices or services across marketplaces.

- **Data portability:** The DMA also contains requirements that gatekeepers enable data portability continuously and in real time, so that end users can transfer their data outside the covered platform service, reducing the burden involved in switching from one platform to another. This

[302] See European Commission, "Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on Contestable and Fair Markets in the Digital Sector and Amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act)," *Official Journal of the European Union*, October 12, 2022, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R1925; and "The Digital Markets Act Promises to Free People from Digital Walled Gardens," EDRi, March 25, 2022, https://edri.org/our-work/the-digital-markets-act-promises-to-free-people-from-digital-walled-gardens.

[303] Anne C. Witt, "Can the EU's Digital Markets Act Rein in Big Tech?" *Conversation*, October 21, 2022, https://theconversation.com/can-the-eus-digital-markets-act-rein-in-big-tech-192373.

[304] Luca Bertuzzi, "The Data Provisions in the EU's Upcoming Big Tech Law," International Association of Privacy Professionals (IAPP), March 22, 2022, https://iapp.org/news/a/the-data-provisions-in-the-eus-upcoming-big-tech-law.

[305] Damien Geradin, Konstantina Bania, Theano Karanikioti, "The Interplay between the Digital Markets Act and the General Data Protection Regulation," August 29, 2022, http://dx.doi.org/10.2139/ssrn.4203907. See page 10.

provision is designed as a complement to the GDPR, and extends to business users of a covered platform in addition to individual end users. Gatekeepers also must implement high-quality technical measures—like APIs—that ensure that data can be ported continuously, in real time and free of charge.[306]

While all of these provisions will have important effects on reducing concentration of power and address the mutually reinforcing dynamics across competition, privacy, and tech policy, there are some limitations to the legal regime outlined under the DMA that indicate competition policy will ultimately need to go further. Most notable is the way the law approaches defining who will be covered by its provisions. The DMA is targeted to the largest firms, which act as gatekeepers. Its definitions require that firms have a large size and impact on the EU internal market, that they control an important gateway for business users to reach end users, and that control be entrenched and durable.[307] The size requirements under this definition would by default likely exclude certain firms (including Twitter), though the provision that the European Commission could select gatekeepers based on more subjective criteria such as market impact could potentially enable Twitter's inclusion.[308] This definitional challenge indicates that who counts as "Big Tech" will likely be a key front for policy battles to come.

**The antitrust bill package before Congress contains a number of structural curbs on firms' power. Though the American Innovation and Choice Online Act and Open App Markets Act are the flagships, the entire package is important for reducing key levers through which tech firms amass power.**

The package of congressional bills intended to supercharge enforcers' ability to push back against concentration in the tech industry received a flurry of attention in 2022, but little movement forward. Built upon a lengthy House investigation into competition in digital markets, the package is designed to introduce a series of curbs on tech firms' power. Two bills form the flagship antitrust measures: the American Innovation and Choice Online Act, or AICOA (HR 3816, S2992), focused on self-preferencing practices used by tech platforms to advantage their own products[309]. It outlines a series of measures that prevent firms from disadvantaging other companies' products and services, and also states that they can't use nonpublic data to advantage their own products. For example, this would prevent Amazon from promoting its own products, such as pushing private-branded goods up in search rankings over those sold by third-party sellers using its Marketplace platform. And the Open App Markets Act would set terms for operation of app marketplaces by prohibiting companies like Apple and Google from prohibiting users from uploading apps from sources other than their proprietary app stores, and requiring companies to let users access payment systems that don't charge the app store commissions.[310]

While these bills have received the bulk of the attention, the other bills constitute important structural and behavioral curbs on tech power: for example, the Platform Competition and Opportunity Act

[306] It may also extend beyond data provided by an end user to cover data that is inferred or derived by the platform. Ibid.; see page 5.
[307] See European Commission, "Digital Markets Act: Rules for Digital Gatekeepers to Ensure Open Markets Enter into Force"; and "The Digital Markets Act Must Do More to Protect End Users' Rights," EDRi, February 11, 2021, https://edri.org/our-work/eu-the-digital-markets-act-must-do-more-to-protect-end-users-rights.
[308] Caitlin Chin, "Elon Musk Bought Twitter Just in Time for a Social Media Crackdown," *Slate*, December 21, 2022, https://slate.com/technology/2022/12/musk-twitter-antitrust-regulation-digital-markets-act.html.
[309] American Innovation and Choice Online Act, S. 2992, 117th Congress (2021–2022), https://www.congress.gov/bill/117th-congress/senate-bill/2992.
[310] Open App Markets Act, S.2710, 117th Congress (2021-2022).

declares acquisitions of direct and potential future competitors unlawful and shifts the burden of proof to dominant platforms to demonstrate that the merger isn't anticompetitive, an *ex ante* measure that would significantly relieve the under resourced merger review teams at the enforcement agencies.[311]

The Ending Platform Monopolies Act would curb interplatform conflicts of interest by forbidding ownership of lines of business that use the covered platform for sale or provision of products and services from offering products that the covered platform requires a business user to purchase in order to access the platform, or that create a conflict of interest.[312] The bill also tackles the complicated web of interfirm board memberships endemic within the industry by forbidding individuals who are in leadership positions at covered platforms from simultaneously serving on the boards of other covered platforms.

The ACCESS Act would reduce barriers to switching between services, requiring covered platforms to maintain interfaces for the secure transfer of user data to other platforms and to enable interoperability with other platforms' systems.[313] It would also provide for the noncommercialization of data by mandating that covered platforms can't use interoperability to collect, use, or share user data except for the purpose of maintaining the privacy and security of the information or to ensure interoperability.[314]

Lastly, the Merger Filing Fee Modernization Act adjusts premerger filing fees to tie them to the Consumer Price Index[315], increasing the resources available to cash-strapped antitrust enforcement agencies; and the State Antitrust Enforcement Venue Act would prohibit firms from requesting state antitrust cases from being transferred to other venues or consolidated into a single multidistrict litigation proceeding[316]. These last two measures were signed into law, even despite significant tech-driven opposition. While these were arguably the most low-hanging, they remain critical wins and indicate movement on antitrust is possible.

The entire package together provides a strong set of levers for addressing concentration of power in the tech industry, if the tenuous bipartisan coalition can see them through. But they're facing an uphill battle: tech firms are bankrolling a ferocious lobbying campaign in opposition to these bills, and thus far have been successful in ensuring they never see the floor of the Senate for a vote.

[311] See Anna Edgerton and Leah Nylen, "Biden's Antitrust Chiefs Seek Funds for Strong Enforcement," *Washington Post*, September 22, 2022, https://www.washingtonpost.com/business/on-small-business/bidens-antitrust-chiefs-seek-funds-for-strong-enforcement/2022/09/21/4d95c6d6-39c0-11ed-b8af-0a04e5dc3db6_story.html; and Federal Trade Commission, "FTC Adjusts its Merger Review Process to Deal with Increase in Merger Filings," August 3, 2021, https://www.ftc.gov/news-events/news/press-releases/2021/08/ftc-adjusts-its-merger-review-process-deal-increase-merger-filings.

[312] Ending Platform Monopolies Act, H.R. 3825, 117th Congress (2021–2022), https://www.congress.gov/bill/117th-congress/house-bill/3825/text.

[313] ACCESS Act of 2021, H.R. 3849, 117th Congress (2021–2022), https://www.congress.gov/bill/117th-congress/house-bill/3849/text.

[314] See Bennett Cyphers and Cory Doctorow, "The New ACCESS Act Is a Good Start. Here's How to Make Sure It Delivers," Electronic Frontier Foundation (EFF), June 21, 2021, https://www.eff.org/deeplinks/2021/06/new-access-act-good-start-heres-how-make-sure-it-delivers; and Bennett Cyphers and Cory Doctorow, "Privacy without Monopoly: Data Protection and Interoperability," Electronic Frontier Foundation (EFF), February 12, 2021, https://www.eff.org/wp/interoperability-and-privacy.

[315] Merger Filing Fee Modernization Act of 2022, H.R. 3843, 117th Congress (2021–2022), https://www.congress.gov/bill/117th-congress/house-bill/3843.

[316] State Antitrust Enforcement Venue Act of 2022, H.R. 3460, 117th Congress (2021–2022), https://www.congress.gov/bill/117th-congress/house-bill/3460.

## The Campaign against Antitrust

- Lobbying by major tech companies surged following the introduction of the bills, increasing by more almost $95 million between 2021 and 2022[317].
- Amazon alone deployed 20 lobbyists to the Senate Judiciary Committee in opposition to the bill.
- 38 lobbyists were used by the four Big Tech firms to campaign against AICOA, 14 of whom worked for the most powerful members of the congressional leadership.[318]
- Over 80 former staffers who worked for Senate Majority Leader Chuck Schumer work directly or indirectly for Big Tech firms, including at least two former chief counsels and one former chief of staff. Schumer has been identified in several analyses as the key impediment to the bills getting a vote.[319]
- Eight complaints have been filed by MEPs against Big Tech companies for engaging in illegal shadow lobbying in the lead-up to the vote on the EU's Digital Markets Act.[320]
- The Connected Commerce Council, which claims to represent five thousand small businesses opposed to the antitrust package, is funded by Amazon and Google; many of the businesses listed as members have never even heard of the group.[321]
- The 12 former national security officials who warned antitrust regulation would threaten US competition with China all have financial ties to tech companies.[322]

[317] Anna Edgerton and Emily Birnbaum, "Big Tech's $95 Million Spending Spree Leaves Antitrust Bill on Brink of Defeat", *Bloomberg,* September 6, 2022

[318] Mike Tanglis, "Lobby, Donate, Hire, Repeat: How Big Tech Is Using the Inside Game to Slow Down Antitrust Reform," Public Citizen, December 16, 2022, https://www.citizen.org/article/lobby-donate-hire-repeat.

[319] Eric Cortellessa, "Schumer Kills Bills Big Tech Feared Most, but Boosts Budgets of Agencies Targeting Them," *Time*, December 22, 2022, https://time.com/6243256/schumer-kills-antitrust-big-tech-bills.

[320] Clothilde Goujard, "Big Tech accused of shady lobbying in EU Parliament," *Politico*, October 14, 2022, https://www.politico.eu/article/big-tech-companies-face-potential-eu-lobbying-ban.

[321] Emily Birnbaum, "Group Backed by Tech Giants Claims Thousands of Members. Many Have Never Heard of It," *Politico*, March 30, 2022, https://www.politico.com/news/2022/03/30/connected-commerce-council-amazon-google-lobbying-00021801.

[322] Emily Birnbaum, "12 Former Security Officials Who Warned against Antitrust Crackdown Have Tech Ties," *Politico*, September 22, 2021, https://www.politico.com/news/2021/09/22/former-security-officials-antitrust-tech-ties-513657.

Biometrics & Affect

# Biometric Surveillance Is Quietly Expanding: Bright-Line Rules Are Key

Despite mounting evidence of harm and untested scientific claims, biometric systems are still quietly proliferating and embedding themselves in new domains like cars and the metaverse.

Existing policy approaches based on data protection law, like the GDPR, have proven to be ineffective in preventing some of the most egregious kinds of biometric systems. In this environment, comprehensive bright-line prohibitions on collection and use are key to future-proof policy interventions.

**Biometric technologies are infiltrating new markets like automobiles, workplaces and virtual reality, but they are not always labeled as such. Often relying on flawed technology for purposes it's not well-designed for, the industries making widespread use of biometrics are nevertheless depending on them for sensitive and inappropriate decision-making, such as evaluating a worker's productivity or a driver's attentiveness.**

Biometrics continue to be quietly embedded in software and hardware across a number of domains where many members of the public encounter them daily, without necessarily knowing they are there or consenting to their use.[323]

[323] See Kelly A. Gates, *Our Biometric Future: Facial Recognition Technology and the Culture of Surveillance* (New York: NYU Press, 2011); Alexandro Pando, "Beyond Security: Biometrics Integration Into Everyday Life," *Forbes*, August 4, 2017; and Rob Davies, "'Conditioning an Entire Society': The Rise of Biometric Data Technology," *Guardian*, October 26, 2021.

The technologies are being used across a wide variety of industries and in diverse contexts; for example, the in-cabin monitoring systems used to track delivery drivers integrates emotion recognition systems that claim to monitor driver "attentiveness" and keep tabs on potentially aggressive behavior.[324] Some remote productivity monitoring software uses eye-movement data collected via webcams to ostensibly monitor employee attention.[325] Call center employees' voices, and those of their customers, are tracked using emotion recognition to monitor for changes in tone and pitch that indicate increased levels of anger and frustration, used to propose canned responses for the call center worker.[326] One provider of "mobile neuroinformatics solutions" purports to measure workers' cognitive state and then provide feedback on their 'cognitive performance and needs'.[327] Across these examples, bodily signals are being used as a proxy to detect characteristics such as "attentiveness" and "aggression," often without clear evidence they are fit for the purpose.[328]

The science does not support the commercialization of many such systems,[329] with plenty of evidence indicating that they lack reliability and validity for the purposes they are currently being used for.[330] Evidence also suggests that they can lead to discriminatory effects.[331] But instead of a reduction in use following significant attention to these harms, we see proposals being unveiled for even more far-reaching uses of hypothetical systems: for example, a video recently shown at Davos touted the purported uses of "brain-wave tracking" to encourage workers to be more focused and productive.[332]

The automotive industry is another key front through which biometrics are being embedded without necessarily being labeled as such. The company Affectiva, which became infamous for releasing an emotion recognition API that claimed to read interior emotional states from facial expressions,[333] has pivoted following its acquisition by SmartEye,[334] a provider of driver monitoring systems and eye-tracking technology, to focus on in-cabin monitoring and automotive technology.[335] Its systems claim to use cameras and sensors to detect fatigue and distraction through collecting data via in-vehicle cameras, an increasingly crowded space occupied by a handful of companies offering similar technology such as Seeing Machines,[336] Cerence,[337] and Eyeris.[338]

[324] See Karen Levy, *Data Driven: Truckers, Technology, and the New Workplace Surveillance* (Princeton: Princeton University Press, 2022); and Lauren Kaori Gurley, "Amazon's AI Cameras Are Punishing Drivers for Mistakes They Didn't Make," *Motherboard*, September 20, 2021; Zephyr Teachout, "Cyborgs on the Highways", *The American Prospect,* December 8, 2022.

[325] Darrell M. West, "How Employers Use Technology to Surveil Employees," Brookings Institution, January 5, 2021.

[326] See, e.g., "The Stakes of Human Interaction Have Never Been So High," Cogito, n.d., accessed March 3, 2023.

[327] Cynthia Khoo, "Re: Notice of Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies — Comments of Center on Privacy & Technology at Georgetown Law", January 15, 2022.

[328] Luke Stark and Jevan Hutson, "Physiognomic Artificial Intelligence," *Fordham Intellectual Property, Media and Entertainment Law Journal* 32, no. 4 (2022): 922–978.

[329] See Lisa Feldman Barrett, Ralph Adolphs, Stacy Marsella, Aleix M. Martinez, and Seth D. Pollak, "Emotional Expressions Reconsidered: Challenges to Inferring Emotion From Human Facial Movements," *Psychological Science in the Public Interest* 20, no. 1 (2019); and Lisa Feldman Barrett, "Inferring Emotions from Physical Signals," Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses, Federal Register Notice 86 FR 56300, January 15, 2022. For a comparative lens on Chinese-developed technologies with similarly flawed scientific validity, see also "Emotional Entanglement: China's Emotion Recognition Market and Its Implications for Human Rights," Article 19, January 2021.

[330] Luke Stark and Jesse Hoey, "The Ethics of Emotion in Artificial Intelligence Systems," *FAccT '21: Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency* (March 2021): 782–793.

[331] See Rosa Wevers, "Unmasking Biometrics' Biases: Facing Gender, Race, Class and Ability in Biometric Data Collection," *TMG Journal for Media History* 21, no. 2 (2018): 89–105; Natasha Lomas, "UK Watchdog Warns against AI for Emotional Analysis, Dubs 'Immature' Biometrics a Bias Risk," TechCrunch, October 26, 2022; Barrett, Adolphs, Marsella, Martinez, and Pollak, "Emotional Expressions Reconsidered"; Sanjana Varghese, "The Junk Science of Emotion-Recognition Technology," *Outline*, October 21, 2019.

[332] Hamilton Nolan, "A World in Which Your Boss Spies on Your Brainwaves? That Future Is Near," *Guardian*, February 9, 2023.

[333] "How It Works," Affectiva, accessed March 3, 2023.

[334] "Smart Eye Acquires Affectiva to Solidify Stronghold on Interior Sensing Market," Business Wire, May 25, 2021.

[335] "Driver Monitoring System: Intelligent Safety Features Detecting Driver State and Behavior," Smart Eye, accessed March 3, 2023.

[336] "Automotive: We Exist to Get Everyone Home Safely," Seeing Machines, accessed March 3, 2023.

[337] Cerence, accessed March 3, 2023.

[338] Eyeris, accessed March 3, 2023.

Such uses carry all of the flaws outlined in the previous section and then some, such as what it will mean for drivers if their "attentiveness" or "aggression" data is shared with insurers or law enforcement authorities.[339] And unique features of the automotive technology ecosystem indicate there are additional concerns to be raised around how Big Tech firms are positioned to benefit from their use. For years, carmakers sought to keep their distance from Big Tech companies, opting instead to contract with smaller companies or develop their own technology in-house to retain greater control over the lucrative streams of data that can be collected on drivers.[340] This has changed: automakers are entering into multiyear partnerships with Big Tech firms that enable deep integration with car hardware systems.[341] For example, Google's Android has become so dominant in the auto ecosystem that the industry standards group the Connected Vehicles Systems Alliance announced it is working to create international standards for car software integration with Android.[342]

Concerns over this rapid expansion by Big Tech companies into the automotive sector are articulated in several letters sent from Congress to FTC Chair Lina Khan and DOJ Assistant Attorney General Jonathan Kanter asking their respective agencies to intervene given the risk that this data could be abused.[343] Moreover, a letter signed by 28 civil society and advocacy organizations urged Congress to act to ensure Big Tech firms are not able to expand their dominance to the automotive market.[344] As elsewhere, strong curbs on the expansion of biometric technologies in the automotive sector would have beneficial impacts on curbing the expansion of concentrated tech power. We see a similar pattern playing out in the augmented/virtual reality market, where companies like Meta are well positioned to build on their data advantage through the influx of a much wider range of new bodily information about consumers made possible through the addition of hardware such as headsets.[345]

[339] Gautham Nagesh, "Eye-Tracking Technology for Cars Promises to Keep Drivers Alert," *Wall Street Journal*, September 9, 2016.
[340] Jacob Kastrenakes, "Why Carmakers Want to Keep Apple and Google at Arm's Length," *Verge*, January 13, 2017.
[341] See Omer Keilaf, "Automakers Partner With Tech Companies To Drive Supply Chain Innovation," *Forbes*, July 28, 2020; Alex Koster, Aakash Arora, and Mike Quinn, "Chasing the Software-Defined Dream Car," Boston Consulting Group (BCG), February 18, 2021; "Tech giants boost partnerships in auto sector," *Automotive News*, September 12, 2019.
[342] Leah Nylen, "Big Tech's Next Monopoly Game: Building the Car of the Future," *Politico*, December 26, 2021.
[343] See Elizabeth Warren to Lina M. Khan and Jonathan Kanter, November 1, 2022; and Jamie Raskin to Lina Khan and Jonathan Kanter, April 1, 2022.
[344] Accountable Tech, American Economic Liberties Project, American Family Voices, Athena, Atwood Center, Blue Future, Demand Progress, Fight for the Future, Institute for Local Self-Reliance, International Brotherhood of Teamsters, IronPAC, Jobs with Justice, Libraries without Borders, Main Street Alliance, Media Alliance, Ocean Futures Society, Open Media and Information Companies Initiative, Organic Consumers Association, The Other 98%, Our Revolution, People's Parity Project, Progress America, Public Citizen, Regeneration International, Revolving Door Project, RootsAction.org, Surveillance Technology Oversight Project, and United We Dream to Amy Kobuchar, David N. Cilcilline, Jonathan Kanter, and Lina Khan, January 25, 2022, https://s3.amazonaws.com/demandprogress/images/Big_Tech_Auto_Letter.pdf.
[345] Veronica Irwin, "Meta Is Looking into Eye-Tracking and Product Placement to Make Money in the Metaverse," *Protocol*, January 18, 2022; Tom Wheeler, "If the Metaverse Is Left Unregulated, Companies Will Track Your Gaze and Emotions," *Time*, June 20, 2022; "Privacy and Autonomy in the Metaverse," Princeton University Library, video, 1:04:12, November 15, 2022.

**Policy frameworks directed at biometric surveillance should ensure they are future-proof against these changing forms and use cases of biometric data. This entails defining biometric systems to explicitly include those designed for inference or analysis (even when they don't uniquely identify the user).**

**While affect recognition appears particularly ripe for a strict ban, there is a rising drumbeat of consensus in favor of prohibiting the use of biometric systems wholesale, given the unjustifiable risks associated with any collection and storage of biometric data.**

Across these examples of workplace and automotive uses of biometric technology, it's clear that expansion is continuing but taking on new form: integration of "facial recognition" technologies is no longer the headline when biometric systems are being deployed, and instead these systems are being described as "safety features" or methods for measuring "productivity."[346] They are also being deployed using methods that may not be immediately obvious or apparent to consumers, and in contexts in which consent is essentially meaningless.

This confusion has policy implications: it allows these emergent systems to escape regulatory scrutiny. Biometric data is widely accepted as a category of "sensitive personal data," and subject to stricter standards of consent and proof of necessity compared to other kinds of personal data. However, most existing legal approaches to regulating biometrics adopt a narrow definition of the term that is conditional on the ability and use of the bodily information to confirm or establish a person's official identity.[347] Some technical literature uses the term "soft biometrics" to define the process of "categorizing information about bodily traits where a person may not be identified in the process."[348] On the one hand, many of these newer systems rely on data (such as iris scans or voice data) that could theoretically be used to confirm or establish identity even though their purpose is more oriented toward evaluation (for, eg., eye tracking or voice capture in the automobile or in an AR/VR context).[349] On the other hand, a range of data signals may not be able to uniquely identify an individual on their own but still reveal potentially sensitive inferences about a person, and should be afforded higher levels of protection.[350]

Evolving policy approaches must adapt to this market evolution. The White House Office of Science and Technology Policy Request For Information on biometric technologies, for example, helpfully defines the term *biometrics* beyond identification to include technologies exclusively directed at the "*inference* of emotion, disposition, character, or intent" and specifically cites keystroke patterns as an example.[351]

This underscores the importance of developing future-proof definitions of biometrics as well as bright-line rules that make clear where certain contexts of use are inappropriate and where certain categories of technology should not be available for commercial development in any instance. One area that is already ripe for such a bright-line prohibition is emotion or affect recognition: public views on

[346] See Stephanie Condon, "Google Expands Virtual Cards to American Express Customers," ZDNET, February 7, 2023; and "The Benefits of Biometric Technology for Workplace Safety," Work Health Solutions, accessed March 3, 2023.
[347] AI Now Institute, *Regulating Biometrics: Global Approaches and Urgent Questions*, September 2020.
[348] See Unsang Park and Anil K. Jain, "Face Matching and Retrieval Using Soft Biometrics," *IEEE Transactions on Information Forensics and Security* 5, no. 3 (September 2010): 406–415; and Antitza Dantcheva, Petros Elia, and Arun Ross, "What Else Does Your Biometric Data Reveal? A Survey on Soft Biometrics," *IEEE Transactions on Information Forensics and Security* 11, no. 3 (March 2016): 441–467.
[349] See Khari Johnson, "Meta's VR Headset Harvests Personal Data Right off Your Face," *Wired*, October 13, 2022; and Janus Rose, "Eye-Tracking Tech Is Another Reason the Metaverse Will Suck," *Motherboard*, March 10, 2022.
[350] Examples include heart rate monitoring, perspiration, and gait tracking, among others.
[351] "Notice of Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies," *Federal Register*, October 8, 2021.

affect recognition have largely soured in response to research documenting the many failures of emotion-recognition systems to live up to the claims companies are making about them.[352] Advocacy organizations have called for affect recognition to be explicitly banned by the EU's upcoming AI Act under the highest risk category of "unjustifiable risks."[353] And the UK Information Commissioner's Office (ICO) also issued a warning against the use of these systems, highlighting that the risks of using emotion recognition outweighs the opportunities.[354] In a recent statement, the ICO's deputy commissioner, Stephen Bonner, said: "As it stands, we are yet to see any emotion AI technology develop in a way that satisfies data protection requirements, and have more general questions about proportionality, fairness and transparency in this area."[355] Recognizing these policy headwinds, in June 2021, Microsoft announced it would stop providing "open-ended API access" to emotion-recognition technology based on "the lack of scientific consensus on the definition of 'emotions,' the challenges in how inferences generalize across use cases, regions, and demographics, and the heightened privacy concerns around this type of capability."[356]

Alongside a slew of city-and-state-level bans targeting law enforcement use of facial recognition in the US,[357] a louder chorus of voices supports a ban on biometrics in particular domains or use cases, such as the collection of biometrics from children,[358] in educational settings,[359] and for certain types of biometrics deemed "high risk" in the workplace.[360] In the EU, there is momentum from advocacy organization around prohibiting "biometric mass surveillance"[361] mechanisms such as live facial recognition systems used by law enforcement or mass scraping to build biometric databases like Clearview AI.

But with more than a decade of advocacy around the potential harms of biometric systems, including recent high-profile incidents that underscore the unjustifiable and potentially devastating consequences of bodily data being misused or weaponized against individuals and communities,[362] there's greater momentum around a more comprehensive ban on the creation and use of such databases.[363] While the dangers of allowing facial recognition has received particular attention[364] given the ability to capture face data "in the wild," and the ubiquity of face images on the web, these arguments increasingly apply to other biometrics like voice or even gait (how a person walks) and, importantly, to commercial contexts in addition to law enforcement use.

[352] See Kate Crawford, "Artificial Intelligence Is Misreading Human Emotion," *Atlantic*, April 27, 2021; Angela Chen and Karen Hao, "Emotion AI researchers say overblown claims give their work a bad name," *MIT Technology Review*, February 14, 2020; Jeremy Kahn, "HireVue Drops Facial Monitoring amid A.I. Algorithm Audit," *Fortune*, January 19, 2021; and Kyle Wiggers, "New Startup Shows How Emotion-Detecting AI Is Intrinsically Problematic," VentureBeat, January 17, 2022.

[353] Access Now, European Digital Rights (EDRi), Bits of Freedom, Article 19, and IT-Pol, "Prohibit Emotion Recognition in the Artificial Intelligence Act," May 2022.

[354] Information Commissioner's Office (ICO), "'Immature Biometric Technologies Could Be Discriminating against People' Says ICO in Warning to Organisations," October 26, 2022.

[355] Ibid.

[356] See James Vincent, "Microsoft to Retire Controversial Facial Recognition Tool That Claims to Identify Emotion," Verge, June 21, 2022; Natasha Crampton, "Microsoft's Framework for Building AI Systems Responsibly," Microsoft (blog), June 21, 2022.

[357] Jameson Spivack and Clare Garvie, "A Taxonomy of Legislative Approaches to Face Recognition in the United States," *Regulating Biometrics: Global Approaches and Urgent Questions*, AI Now Institute, September 2020.

[358] Lindsey Barrett, "Ban Facial Recognition Technologies for Children—And for Everyone Else," *Boston University Journal of Science and Technology Law* 26, no. 2 (2020): 223–285.

[359] Nila Bala, "The Danger of Facial Recognition in Our Children's Classrooms," Duke Law & Technology Review 18, no. 1 (2020): 249–267.

[360] Worker Rights: Workplace Technology Accountability Act, A.B. 1651 (California Legislature, 2021–2022 Regular Session), January 13, 2022.

[361] The Greens, "Fighting for a Ban on Mass Surveillance in Public Spaces"; Access Now, "Ban Biometric Surveillance", June 7, 2022.

[362] See Eileen Guo and Hikmat Noori, "This is the real story of the Afghan biometric databases abandoned to the Taliban," *MIT Technology Review*, August 30, 2021; and Kashmir Hill, "The Secretive Company That Might End Privacy as We Know It," *New York Times*, January 18, 2020.

[363] See Access Now, "Open Letter Calling for a Global Ban on Biometric Recognition Technologies That Enable Mass and Discriminatory Surveillance," June 7, 2021; and Algorithm Watch, "Open Letter Calling for a Global Ban on Biometric Recognition Technologies That Enable Mass and Discriminatory Surveillance," 2021.

[364] See Luke Stark, "Facial Recognition Is the Plutonium of AI," *XRDS: Crossroads, the ACM Magazine for Students* 25, no. 3 (Spring 2019): 50–55, and Evan Selinger and Woodrow Hartzog, "What Happens When Employers Can Read Your Facial Expressions?" *New York Times*, October 17, 2019.

Global Digital Trade

# International “Digital Trade” Agreements: The Next Frontier

International trade agreements, typically negotiated in secret and without public deliberation, could prematurely deter or undercut ongoing efforts to regulate the tech industry.

Negotiations on a possible Indo-Pacific Economic Framework and trade talks with Latin American and other countries must preserve this policy space and set a more progressive baseline for digital policy.

**Trade agreements include binding international rules that limit the parameters of how governments can regulate commercial firms. Because of the secrecy of the negotiations and their relative immunity to public political pressure, they have become a focus for intense tech industry lobbying for preferential treatment.**

**“Digital trade” is fast emerging as the next battleground where trade rules could function to prematurely deter or undercut ongoing regulatory efforts around data privacy, algorithmic accountability, and competition in the tech industry.**

International trade law includes a sprawling body of legal agreements: binding multilateral rules applicable to all 164 member countries of the World Trade Organization (WTO), as well as bilateral or regional agreements between two or more countries that determine the rules of the road for how the cross-border exchange of products and services is regulated as well as how foreign firms and their services can be regulated by a host government. [365] International trade agreements that extend beyond traditional matters, such as tariffs and quotas, are a relatively recent creation, having only become widespread at the end of the twentieth century, together with, and very much espoused by, the neoliberal order then emerging.[366] Per this ideology, "free trade" and the removal of "barriers to trade" between countries will result in growing the "global pie," making all parties better off.[367] Under this account, protectionism of any kind, or policies that directly (or—crucially—indirectly) prioritize domestic workers or businesses, or disadvantage foreign ones, are misguided and eventually stifle growth and shrink both the domestic and global economy.[368]

This consensus against protectionism is generally operationalized through the reduction of border barriers to trade, most prominently tariffs and quotas, and rules around nondiscrimination, such as the "national treatment" principle, which requires that countries do not treat commerce from other member countries less favorably that they treat their own.[369] For example, the US may not subject Canadian products to stricter regulation than those that US products are subject to.[370] And, unlike many other bodies of international law, not following these rules has punitive consequences: Countries can be sued before the WTO, or under bilateral or regional deals' dispute settlement systems, and sanctions can be imposed until nonconforming domestic policies are removed or changed.[371]

While traditional trade barriers included custom duties and tariffs, more recent trade agreements have strongly emphasized regulation as a potential trade barrier.[372] Over the past few decades, international trade rules have been enforced (by suing countries before the WTO[373] or other trade and investment dispute settlement mechanisms) to resist and successfully defeat national regulation that pursues other non-trade-related policy goals like environmental conservation, public health or the promotion of green industries.[374] In response to this shrinking space for governments to make policy in pursuit of national priorities, advocates for environmental justice, labor, and human rights,[375] as well as countries from the Global South advocating for equitable development opportunities,[376] have fought for "exceptions" to these rules to create room for national-level regulatory moves. This has occurred even

[365] Burcu Kilic and Renata Avila, "The Multilateral Trade System and the World Trade Organization (WTO): Lesson 101," Public Citizen, n.d., accessed March 3, 2023, https://www.citizen.org/article/the-wto-101.

[366] Quinn Slobodian, *Globalists: The End of Empire and the Birth of Neoliberalism* (Cambridge, MA: Harvard University Press, 2018)..

[367] Harlan Grant Cohen, "What Is International Trade Law For?" *American Journal of International Law* 113, no. 2 (April 2019): 326–346, https://www.cambridge.org/core/journals/american-journal-of-international-law/article/what-is-international-trade-law-for/F8C98A6B262B92A3C97632E402D01EDC.

[368] Benoît Coeuré, "The Consequences of Protectionism," European Central Bank, April 6, 2018, https://www.ecb.europa.eu/press/key/date/2018/html/ecb.sp180406.en.html.

[369] "Principles of the Trading System," World Trade Organization, accessed March 3, 2023, https://www.wto.org/english/thewto_e/whatis_e/tif_e/fact2_e.htm.

[370] Timothy Meyer, "The Political Economy of WTO Exceptions," *Washington University Law Review* 99, no. 4 (2022): 1299–1370, https://scholarship.law.vanderbilt.edu/cgi/viewcontent.cgi?article=2280&context=faculty-publications.

[371] Kilic and Avila, "The Multilateral Trade System and the World Trade Organization (WTO)." Some of these agreements also empower foreign investors to privately enforce the terms through a process called "investor-state dispute settlement," which grants corporations the ability to sue governments before a panel of three private-sector lawyers picked by the parties. These lawyers can award the corporations unlimited sums to be paid by taxpayers, including for the loss of expected future profits and their decisions are not subject to appeal, see Jane Kelsey and Lori Wallach, ""Investor-State" Disputes in Trade Pacts Threaten Fundamental Principles of National Judicial Systems', *Citizen*, April 2012, https://www.citizen.org/wp-content/uploads/isds-domestic-legal-process-background-brief.pdf.

[372] Burcu Kilic, *Shaping the Future of Multilateralism—Digital Trade Rules: Big Tech's End Run around Domestic Regulations* (Washington, DC: Heinrich-Böll-Stiftung, 2021) https://eu.boell.org/en/2021/05/19/shaping-future-multilateralism-digital-trade-rules-big-techs-end-run-around-domestic.

[373] "Whose WTO Is It, Anyway?" World Trade Organization, accessed March 3, 2023, https://www.wto.org/english/thewto_e/whatis_e/tif_e/org1_e.htm.

[374] See Barbara Moens and Karl Mathiesen, "Trade Partners See Red over Europe's Green Agenda," *Politico*, January 16, 2023, https://www.politico.eu/article/eu-green-agenda-has-its-trading-partners-seeing-red-climate-neutrality; and David Henderson, "Unlawful Trade Barrier Warning over Bottle Return Scheme," BBC, February 8, 2023, https://www.bbc.co.uk/news/uk-scotland-64563015.

[375] Larry A. DiMatteo, Kiren Dosanjh, Paul L. Frantz, Peter Bowal, and Clyde Stoltenberg, "The Doha Declaration and Beyond: Giving a Voice to Non-Trade Concerns Within the WTO Trade Regime," *Vanderbilt Journal of Transnational Law* 36, no. 1 (January 2003): 95–160, https://scholarship.law.vanderbilt.edu/cgi/viewcontent.cgi?article=1597&context=vjtl.

[376] See B.S. Chimni, "Third World Approaches to International Law: A Manifesto," *International Community Law Review* 8, no. 1 (2006): 3–27, https://www.jnu.ac.in/sites/default/files/Third%20World%20Manifesto%20BSChimni.pdf.

as the prevailing exception language and its interpretation led to the demonization of public interest policies, which are then scrutinized within the current trade regime for being protectionism in disguise or arbitrarily discriminatory.[377]

"Digital trade" or trade agreements that apply to technology-related products, services and firms are emerging as the next battleground where trade rules could function to deter or undercut global regulatory efforts pursuing privacy protection, algorithmic accountability, and competition objectives, among other things.[378] In the US, this risk is heightened in the current moment: with no federal regulation on data privacy, digital markets competition, and algorithmic accountability, but significant political momentum across these areas,[379] any trade agreements signed by the US that further entrench and expand the privileges the tech industry enjoys could end up prematurely cutting off the opportunity to make such interventions.

The tech industry has been quick to recognize and exploit trade policy as a vehicle for regulatory influence. Negotiation of the Trans-Pacific Partnership (TPP) set the initial blueprint for the Big Tech policy agenda for digital trade.[380] The TPP was a highly contested agreement between the US and 11 Pacific Rim countries.[381] It was the first trade agreement with a strong emphasis on digital trade. TPP negotiations started in 2008 and a deal was signed in early 2016) behind closed doors and with significant evidence of lobbying by Big Tech,[382] foreclosing the possibility of any robust public input.[383] There was never a U.S. congressional majority in support of the deal. But in 2018 the other 11 countries suspended a few of the most extreme provisions and enacted it rebranded as the Comprehensive Progressive Trans-Pacific Partnership. The TPP chapter covering digital trade, which became public in 2016 shortly before signing, provided an initial blueprint for the Trump administration to provide further industry privileges in the 2019 US-Mexico-Canada Agreement (USMCA).[384] This agenda reflects the standard policy positions advocated for by large tech companies in national debates, including limiting any restrictions on cross-border data flows, an absolute restriction on data localization (requirements that data be stored within the country) and locking in and exporting to other countries Section 230's limits on online platform liability. Also included are strict protections against government access to source code. In USMCA this protection extends even to detailed descriptions of algorithms. The effect of this provision is to label many otherwise facially neutral policies as illegal trade barriers. While they apply to domestic and foreign firms equally, they may have a bigger impact on certain firms because they are larger, not because of their nationality.[385]

The TPP set a dangerous precedent: the tech industry now looks to trade agreements as an arena where they can lobby to establish policy positions globally, bypassing public scrutiny, before these

[377] Meyer, "The Political Economy of WTO Exceptions."

[378] Kilic, *Shaping the Future of Multilateralism*.

[379] See ACCESS Act of 2021, H.R. 3849, 117th Congress (2021–2022), https://www.congress.gov/bill/117th-congress/house-bill/3849/text; American Innovation and Choice Online Act, S. 2992, 117th Congress (2021–2022), https://www.congress.gov/bill/117th-congress/senate-bill/2992/text; and Worker Rights: Workplace Technology Accountability Act, .B. 1651 (California Legislature, 2021–2022 Regular Session), January 13, 2022, https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202120220AB1651.

[380] See Kilic, *Shaping the Future of Multilateralism*; and Peter Baker, "Trump Abandons Trans-Pacific Partnership, Obama's Signature Trade Deal," *New York Times*, January 23, 2017, https://www.nytimes.com/2017/01/23/us/politics/tpp-trump-trade-nafta.html.

[381] Kevin Granville, "What Is TPP? Behind the Trade Deal That Died," *New York Times*, January 23, 2017, https://www.nytimes.com/interactive/2016/business/tpp-explained-what-is-trans-pacific-partnership.html.

[382] See Wendy Li, "Regulatory Capture's Third Face of Power", Socio-Economic Review, 2023, Vol. 00, 1-29, https://sociology.wisc.edu/2023/02/07/regulatory-captures-third-face-of-power-by-wendy-li-2023/.

[383] Mark Wu, "US Should Not Negotiate Free Trade behind Closed Doors," *Financial Times*, May 26, 2015, https://www.ft.com/content/28432090-03b3-11e5-a70f-00144feabdc0.

[384] David A. Gantz, "The USMCA: Updating NAFTA by Drawing on the Trans-Pacific Partnership," Baker Institute for Public Policy, February 21, 2020, https://www.bakerinstitute.org/research/usmca-updating-nafta-drawing-trans-pacific-partnership.

[385] Thomas Streinz, "Digital Megaregulation Uncontested? TPP's Model for the Global Digital Economy," Guarini Institute for Global Legal Studies: Global Law & Tech, August 13, 2019, https://www.guariniglobal.org/gglt-publications/2022/6/8/digital-megaregulation-uncontested-tpps-model-for-the-global-digital-economy.

issues are democratically deliberated in national contexts. A March 2023 analysis by Rethink Trade pointed to a long list of ways in which the TPP and USMCA provisions directly contradict emerging policy positioning that has been subsequently put forth by the Biden administration.[386] This acts as a potential deterrent against renewed efforts by the US (or any signatory) government to regulate the tech industry: in order to pass such policies, which might clash with existing or forthcoming trade agreements, they would have to justify why these don't violate international obligations or fall under stated exceptions.

Looking ahead, Katherine Tai, the US Trade Representative (USTR) under the Biden administration, has suggested that the US will now take a different approach to trade from the one pursued under the TPP and USMCA.[387] In fact, she has repeatedly advocated for a trade agenda that centers consumer and worker interests,[388] signaling an opportunity to reconceptualize trade agreements as a vehicle for setting a higher progressive baseline in favor of greater policy protections, and not just as an anti-regulation tool for industry. All eyes are on the upcoming Indo-Pacific Economic Framework (IPEF), a trade agreement between the US and 13 countries in the Asian Pacific region (widely heralded as a US attempt to counter Chinese influence in the region[389]) as a site where this new orientation could play out.[390]

While the text of the IPEF is still not public, progressive trade groups have helpfully identified potentially problematic digital trade issues that are likely to come up including prohibitions on government oversight of data flows for privacy or data security purposes and government regulation of where data can be processed or stored, overly expansive nondiscrimination terms as well as expansive and absolute source code and algorithmic secrecy guarantees that could limit government AI oversight.

### Nondiscrimination prohibitions in trade agreements should not be used to protect US Big Tech companies from competition regulation abroad. Such provisions must be crafted to leave policy space for laws aimed at enhancing competition, even where they might disproportionately impact US Big Tech firms.

The TPP and USMCA have a broadly worded "nondiscrimination" requirement that could be interpreted as restricting member countries from enacting policy that, while neutral on its face, effectively has a greater impact on firms from a particular country. In the context of antitrust or other pro-competition regulation, this could mean therefore that competition regulation that disproportionately impacts U.S.

[386] Daniel Rangel and Lori Wallach, "International Preemption by "Trade" Agreement: Big Tech's Ploy to Undermine Privacy, AI Accountability, and Anti-Monopoly Policies", *Rethink Trade*, March 15, 2023, https://rethinktrade.org/reports/international-preemption-by-trade-agreement/.

[387] See Claude Barfield, "US Indo-Pacific Policy Prioritises Security over Economics," East Asia Forum, February 10, 2023, https://www.eastasiaforum.org/2023/02/10/us-indo-pacific-policy-prioritises-security-over-economics; and "US Trade Representative Tai hints at new Asian economic framework - NHK," Reuters, November 18, 2021, https://www.reuters.com/world/asia-pacific/us-trade-representative-tai-hints-new-asian-economic-framework-nhk-2021-11-18.

[388] Jeanna Smialek, "Ambassador Tai Outlined Biden's Goal of Worker-Focused Trade Policy," *New York Times*, June 10, 2021, https://www.nytimes.com/2021/06/10/business/economy/us-trade-katherine-tai.html.

[389] See "Indo-Pacific Economic Framework Holds Value, but It's Unclear If It Will Counter China's Influence Says Senior Economist David Dapice," Ash Center, Harvard Kennedy School, n.d., accessed March 3, 2023, https://ash.harvard.edu/indo-pacific-economic-framework-holds-value-it%E2%80%99s-unclear-if-it-will-counter-china%E2%80%99s-influence; Enda Curran and Michelle Jamrisko, "Understanding IPEF and How It Counters China's Clout," Bloomberg, May 23, 2022, https://www.bloomberg.com/news/articles/2022-05-23/how-the-us-and-china-duel-to-gain-trade-clout-in-asia-quicktake; and Andrew Haffner, "Biden Launches Economic Framework Aimed at Countering China," Al Jazeera, May 23, 2022, https://www.aljazeera.com/economy/2022/5/23/biden-launches-economic-framework-aimed-at-countering-china.

[390] Public Citizen, "IPEF Launch Suggests Departure from TPP but Also Raises Red Flags," press release, May 23, 2022, https://www.citizen.org/news/ipef-launch-suggests-departure-from-tpp-but-also-raises-red-flags.

Big Tech companies (because of their size, scale, and data advantages) could be seen as violating the nondiscrimination *diktat* of the trade agreement.

This risk is not hypothetical. We've already seen Apple and Google wield this argument in the context of South Korea's 2021 law targeting anticompetitive app store policies, on the grounds that it has a discriminatory effect because of its disparate impact on US firms.[391] Rethink Trade also published a report that reveals a pattern of this kind of corporate lobbying using broad "nondiscrimination" arguments to undermine other countries' competition regulation.[392] Other non-Big Tech companies in the industry are also chiming in: in a recent letter to the USTR titled "Don't Let Big Tech Manipulate Trade Policy to Kill Competition," the Coalition on App Fairness, whose larger members include Spotify and Epic Games, urged the USTR not to follow the USMCA/TPP approach and ensure that the IPEF does not "provides a basis for US Big Tech monopolies to attack legitimate anti-monopoly policies in other countries as 'illegal trade barriers.'"[393] These efforts all point to the wave of competition-focused regulation being proposed in the US, along with the Biden administration's declaration not to "tolerate domestic monopolies" as further reason not to entrench contradictory positions in global trade fora.

Much of the impact of the nondiscrimination provision will be determined by its precise wording. In the South Korea app store case, Apple and Google's complaint to the US government wasn't a credible legal threat given that the Korea-US trade agreement (KORUS) did not have the TPP/USMCA-style of nondiscrimination clause and so the argument remained conceptual. This only underscores the importance of ensuring carefully tailored language that avoids the pitfalls of the TPP in IPEF and other future agreements.[394] Rethink Trade draws on the language in KORUS to propose a variation that preserves space for such pro-competition policy, by clarifying that a country will not be in violation "merely because" it results in differential effects on a particular country's products and instead must have the "objective or predominant intent to afford protection."[395]

### Expansive and absolute-secrecy guarantees for source code and algorithms in trade agreements could undermine the direction of algorithmic accountability policy in the US and globally where there is a general movement towards mandating more proactive and continuous monitoring of AI systems.

Expansive and absolute-secrecy guarantees for source code and algorithms are another key feature of the industry-backed USMCA/TPP approach. These provisions are justified as preventing the forced transfer of software trade secrets as a condition for market access (a concern animated primarily by Chinese actions in the past),[396] but the broadly worded protections effectively risk preventing government oversight over algorithms wholesale, and especially so when they involve proactive monitoring and are not in response to a specific court order.

[391] David McCabe and Jin Yu Young, "Apple and Google's Fight in Seoul Tests Biden in Washington," *New York Times*, August 23, 2021, https://www.nytimes.com/2021/08/23/technology/apple-google-south-korea-app-store.html.
[392] Daniel Rangel, Taylor Buck, Erik Peinert, and Lori Wallach, "'Digital Trade' Doublespeak: Big Tech's Hijack of Trade Lingo to Attack Anti-Monopoly and Competition Policies," Rethink Trade, November 2022, https://rethinktrade.org/wp-content/uploads/2022/11/20221101-AELP-DocLayout-v7.pdf.
[393] Rick VanMeter to Katherine Tai and Gina Raimondo, January 11, 2023, https://appfairness.org/wp-content/uploads/2023/01/20230111_USTR-IPEF-CAF-Letter.pdf.
[394] Rethink Trade's submission on IPEF (forthcoming; on file with author).
[395] Ibid.
[396] Keith Bradsher, "How China Obtains American Trade Secrets," *New York Times*, January 15, 2020, https://www.nytimes.com/2020/01/15/business/china-technology-transfer.html.

This contradicts the direction of algorithmic accountability policy globally (including multiple proposals in the US), which is moving toward more proactive and continuous monitoring of AI systems, especially in sensitive or high-risk domains.[397] Several organizations have pointed out that the USMCA definition of "algorithm" is broad enough to restrict the sharing of even mere descriptions of algorithms with regulators, a key part of algorithmic transparency proposals such as AI registries.[398] This could have impacts across a range of proposals, such as regulatory evaluations of AI (including those addressing worker surveillance), anticompetitive self-preferencing, and bias and discrimination. In their recent testimony, the AFL-CIO, a consortium of American labor unions, argued that any USMCA-style source code/algorithm secrecy provision would operate to "prevent the protection of workers from the excesses of algorithmic management."[399]

Looking forward to IPEF, this issue remains a consistent lobbying priority for the tech industry. In February 2022, the US Chamber of Commerce flagged that a top priority for industry in relation to digital trade was that "companies should not be forced to transfer their technology, including proprietary algorithms, to competitors or governments."[400] A broadly worded protection for source code and algorithms risks seriously undermining efforts around algorithmic accountability both in the US and abroad, and must be prevented.

### Beyond these defensive approaches, there is also potential for the IPEF and forthcoming trade policy to set a more progressive baseline on these issues.

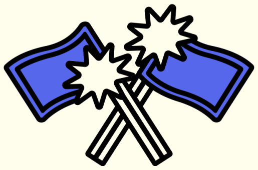
The aspiration toward a more proactive stance is somewhat constrained by the fact that, despite growing momentum, the US lacks enforceable federal policy on issues like privacy, surveillance, digital markets competition, and algorithmic accountability. In the absence of a clear regulatory benchmark, US negotiators do not have direction with respect to a US baseline standard to be promoted in trade pacts. That said, even nonbinding language that highlights the need for global consensus in favor of clear limits on commercial and worker surveillance, algorithmic accountability, and competition regulation would represent a major departure from the TPP/USMCA model—one that opens up the possibility of trade law as a vehicle for pushing forward (rather than against) tech accountability.

[397] See PACT Act, S. 797, 117th Congress (2021–2022), https://www.congress.gov/bill/117th-congress/senate-bill/797/text; Worker Rights: Workplace Technology Accountability Act, A.B. 1651, California Legislature (2021–2022), https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202120220AB1651; European Commission, "Proposal for a Directive of the European Parliament and of the Council on Improving Working Conditions in Platform Work," December 9, 2021, https://ec.europa.eu/social/BlobServlet?docId=24992&langId=en; Algorithmic Accountability Act of 2022, H.R. 6580, 117th Congress (2021–2022), https://www.congress.gov/bill/117th-congress/house-bill/6580/text; European Commission, "The Digital Services Act Package," n.d., accessed March 3, 2023, https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package; and Worker Rights: Workplace Technology Accountability Act, A.B. 1651.

[398] Duncan McCann, *"e-Commerce: Free Trade Agreements, Digital Chapters and the impact on Labour",* ITUC, 2019, https://www.ituc-csi.org/e-commerce-report.

[399] *Hearing on "Opportunities and Challenges for Trade Policy in the Digital Economy," Before the Subcommittee on International Trade, Customs, and Global Competitiveness*, US Senate Finance Committee, 117th Congress, Second Session (November 30, 2022) (Statement of Patrick Woodhall, Policy & Research Director, AFL-CIO Technology Institute), https://www.finance.senate.gov/imo/media/doc/Woodall%20AFL-CIO%20Tech%20Insittute%20Digital%20Trade%20Testimony.pdf.

[400] U.S. Chamber of Commerce, "U.S. Chamber Digital Trade Priorities," n.d., accessed March 3, 2023, https://www.uschamber.com/assets/documents/024211_US_Chamber_Digital_Trade_Priorities_v1.pdf.



US-China AI Race

# AI Policy as Industrial Policy

The so-called “AI race” between the US and China is increasingly used by a constellation of industry and national security actors to push back against regulatory intervention targeting US Big Tech companies. In turn, there has been rapid policy movement towards greater state support for large-scale AI development.

This has surfaced in at least three policy domains: antitrust or pro-competition regulation; data privacy; and industrial policy that increases government support for AI development.

**The rhetoric around the US-China AI race has evolved from a sporadic talking point to an increasingly institutionalized position, represented by collaborative initiatives between government, military, and tech-industry actors and reinforced by legislation and regulatory debates.**

**These initiatives crystallize the notion of AI systems (and the companies that produce them) not merely as commercial products but foremost as strategic national assets.**

In the 2019 AI Now Report, we flagged the emergence of the so-called “AI arms race” between US and China as a lens gaining currency in public discourse.[401] Identifying the loudest proponents of this narrative—predominantly voices from the tech industry and the US defense establishment—illuminated the interests and interlocking power structures that are bolstered by this particular view of technological progress. In the US, it was clear that the so-called “AI race” against China not only kindled

[401] See Kate Crawford, 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*, AI Now Institute, December 2019, https://ainowinstitute.org/AI_Now_2019_Report.pdf; see also Meredith Whittaker, Shazeda Ahmed, and Amba Kak, “China in Global Tech Discourse,” AI Now Institute, Medium, May 27, 2021, https://medium.com/@AINowInstitute/china-in-global-tech-discourse-2524017ca856.

an appetite, across party lines,[402] for increased support of escalated AI development and deployment, but also served to push back against calls for slower, more intentional development and stronger regulatory protections.

Since then, this rhetoric has not just persisted, but has expanded in influence, and is being more deliberately wielded in the policy sphere to advocate for interests aligned with the biggest tech corporations. Efforts to stoke the fear that this is a race (or an "AI-accelerated competition"[403]) in which the US is already lagging behind—or, in the words of the Special Competitive Studies Project (SCSP), an organization chaired by Eric Schmidt, former CEO of Google (now Alphabet), is "perilously and unwittingly close to ceding"[404]—are designed to emphasize urgency and spur policy action.[405] The **timeline** below shows that the AI race against China has evolved from a sporadic talking point to an increasingly institutionalized position, represented by collaborative initiatives between government, military, and tech-industry actors and reinforced by legislation and regulatory debates. We see, for example, the seamless evolution of the congressionally mandated National Security Commission on Artificial Intelligence (NSCAI)[406] to the privately funded SCSP,[407] founded in October 2021, with the same leadership (Eric Schmidt and former NSA official Ylli Bajraktari) and stated goals as the NSCAI. The SCSP explicitly builds on the legacy of the 1956 Rockefeller Cold War Special Studies Project and is framed around adapting Cold War-era thinking to "the age of AI."[408]

These initiatives crystallize the notion of AI (and a growing list of other technologies like 5G, quantum computing, and blockchain) as strategic technologies that must be viewed not merely as commercial products but foremost as strategic national assets, along with the companies that produce them. (The SCSP refers to tech platforms as "tools of statecraft too powerful to ignore."[409]) This logic translates into the policy sphere as a way to push back against regulatory intervention targeting these companies and in pursuit of greater state support for a specific kind of large-scale AI innovation. This is most noticeable in at least three policy domains: antitrust or pro-competition regulation; data privacy regulation; and industrial policy measures that allocate public funding toward AI development.

[402] See 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; Jake Harrington and Riley McCabe, "What the U.S. Innovation and Competition Act Gets Right (and What It Gets Wrong)," Center for Strategic and International Studies (CSIS), July 1, 2021, https://www.csis.org/analysis/what-us-innovation-and-competition-act-gets-right-and-what-it-gets-wrong; and David E. Sanger, Catie Edmondson, David McCabe, and Thomas Kaplan, "Senate Poised to Pass Huge Industrial Policy Bill to Counter China," *New York Times,* June 7, 2021, https://www.nytimes.com/2021/06/07/us/politics/senate-china-semiconductors.html.
[403] National Security Commission on Artificial Intelligence, *Final Report*, 2021, https://nscai.wpenginepowered.com/wp-content/uploads/2021/03/Full-Report-Digital-1.pdf. See page 8.
[404] Special Competitive Studies Project, "Mid-Decade Challenges to National Competitiveness," September 2022, https://www.scsp.ai/wp-content/uploads/2022/09/SCSP-Mid-Decade-Challenges-to-National-Competitiveness.pdf. See page 18.
[405] See Meredith Whittaker and Lucy Suchman, "The Myth of Artificial Intelligence," *American Prospect*, December 8, 2021, https://prospect.org/culture/books/myth-of-artificial-intelligence-kissinger-schmidt-huttenlocher.
[406] The National Security Commission on Artificial Intelligence, accessed March 3, 2023, https://www.nscai.gov. Note that the NSCAI ceased operations on October 1, 2021. Permanent archive of the NSCAI website: https://cybercemetery.unt.edu/nscai/20211005220330/https://www.nscai.gov.
[407] Special Competitive Studies Project, accessed March 3, 2023, https://www.scsp.ai.
[408] See "What We Do," Special Competitive Studies Project, accessed March 3, 2023, https://www.scsp.ai/about/what-we-do/#mission; https://www.rbf.org/about/our-history/timeline/special-studies-project/in-depth; see also Henry Kissinger, Eric Schmidt, and Daniel Huttenlocher, *The Age of AI: And Our Human Future* (New York: Back Bay Books, 2022).
[409] Special Competitive Studies Project, "Mid-Decade Challenges to National Competitiveness." See page 22.

**Arguments against antitrust based on the US-China “AI race” are being cynically promoted by industry interests—yet the Biden administration, with its Executive Order on Promoting Competition in the American Economy, offers a clear refutation to this logic: it proposes a competitive tech industry as the clearest path to advocating for the national interest. For those genuinely working toward that goal, competition enforcement is a key part of how we get there.**

In 2019, Sheryl Sandberg (then COO at Facebook) warned that the backlash against American tech companies like her employer ignored that Chinese companies weren't under similar scrutiny: “While people are concerned with the size and power of tech companies, there's also a concern in the United States with the size and power of Chinese companies, and the realization that these companies are not going to be broken up.”[410] Mark Zuckerberg's personal notes for a congressional hearing, photographed by the Associated Press,[411] were even more explicit: “Break up FB? US tech companies key asset for America; break up strengthens Chinese companies.”

As renewed antitrust enforcement and pro-competition regulation gain global momentum,[412] not least in the Biden administration,[413] this defense and its proponents have only grown louder. One version of this argument exploits the bipartisan concern about Chinese economic dominance and warns that anyone considering “dismantling US firms that invest heavily in AI [...] should think twice.”[414] More notable has been the proliferation of a national security-focused rationale for this same argument. In 2021, CCIA, an industry lobby group whose members include Amazon, Apple, Google, Facebook, and others, published a white paper called “National Security Issues Posed by House Antitrust Bills”[415] that canvases several reasons why pro-competition legislation threatens the national interest, including:

- The American Innovation and Choice Online Act[416] would affect companies' ability to resist malicious activity.

[410] Nitasha Tiku, “Big Tech: Breaking Us Up Will Only Help China,” *Wired*, May 23, 2019, https://www.wired.com/story/big-tech-breaking-will-only-help-china.

[411] See Alix Langone, “The Photojournalist Who Took a Picture of Mark Zuckerberg's Notes Reveals Why He Did It,” *Time*, April 11, 2018, https://time.com/5236407/mark-zuckerberg-notes-testimony-photo; and Andrea Woo (@AndreaWoo), “Mark Zuckerberg's notes today, from AP photojournalist Andrew Harnik,” Twitter, April 10, 2018, 8:36 p.m., https://twitter.com/AndreaWoo/status/983866296264810496.

[412] See Sam Shead, “The Walls Are Closing in on Big Tech as Global Regulators Crack Down,” CNBC, December 15, 2020, https://www.cnbc.com/2020/12/15/regulators-crack-down-big-tech-dsa.html; European Commission, “Digital Markets Act: Rules for Digital Gatekeepers to Ensure Open Markets Enter into Force,” press release, October 31, 2022, https://ec.europa.eu/commission/presscorner/detail/en/IP_22_6423; Ivan Mehta, “South Korea to Probe Apple and Google Over In-App Payment Rule Break,” TechCrunch, August 9, 2022, https://techcrunch.com/2022/08/09/south-korea-to-probe-apple-and-google-over-in-app-payment-rule-break; and Australian Competition & Consumer Commission, “Digital Platform Services Inquiry 2020–25: Project Overview,” n.d., accessed March 3, 2023, https://www.accc.gov.au/focus-areas/inquiries-ongoing/digital-platform-services-inquiry-2020-25.

[413] See White House, “Executive Order on Promoting Competition in the American Economy,” July 9, 2021, https://www.whitehouse.gov/briefing-room/presidential-actions/2021/07/09/executive-order-on-promoting-competition-in-the-american-economy; American Innovation and Choice Online Act, S. 2992, 117th Congress (2021–2022), https://www.congress.gov/bill/117th-congress/senate-bill/2992; and Ending Platform Monopolies Act, H.R. 3825, 117th Congress (2021–2022), https://www.congress.gov/bill/117th-congress/house-bill/3825/text.

[414] See Theadora Soter, “Direction of Antitrust Enforcement Could Harm American Global Competitiveness, Says Head of Think Tank,” Broadband Breakfast, April 11, 2022, https://broadbandbreakfast.com/2022/04/direction-of-antitrust-enforcement-could-harm-american-global-competitiveness-says-head-of-think-tank; Robert D. Atkinson, “Why the United States Needs a National Advanced Industry and Technology Agency,” Information Technology & Innovation Foundation (ITIF), June 17, 2021, https://itif.org/publications/2021/06/17/why-united-states-needs-national-advanced-industry-and-technology-agency; Robert D. Atkinson, “Advanced Industries Are Essential for U.S. Competitiveness,” Information Technology & Innovation Foundation (ITIF), February 3, 2023, https://itif.org/publications/2023/02/03/advanced-industries-are-essential-for-us-competitiveness; and Ian Clay and Robert D. Atkinson, “Wake Up, America: China Is Overtaking the United States in Innovation Capacity,” Information Technology & Innovation Foundation (ITIF), January 23, 2023, https://itif.org/publications/2023/01/23/wake-up-america-china-is-overtaking-the-united-states-in-innovation-capacity.

[415] Computer & Communications Industry Association, “National Security Issues Posed by House Antitrust Bills,” September 2021, https://ccianet.org/wp-content/uploads/2021/09/CCIA-KS-NatSec-White-Paper.pdf.

[416] American Innovation and Choice Online Act, S. 2992.

- The Augmenting Compatibility and Competition by Enabling Service Switching (ACCESS) Act[417] could impact national security by compelling leading US tech companies to share data and ensure interoperability with other organizations, including foreign entities.
- The Platform Competition and Opportunity Act[418] would severely restrict US companies' ability to make mergers and acquisitions but would not apply to foreign rivals.
- The Ending Platform Monopolies Act[419] would also disadvantage US firms compared to their international competitors due to restrictions on mergers and acquisitions.

These lobbyists argue that together, these bills would threaten national security by risking the misuse of US intellectual property and data; reducing US law enforcement's access to effective data; reducing the US's ability to combat foreign misinformation; impeding cybersecurity efforts; giving foreign companies an advantage over US companies without any reciprocity; and "undermining U.S. tech leadership."[420]

This lobbying attempt was followed by a similarly worded letter[421] from former senior defense officials. A subsequent *Politico* investigation exposed that all twelve signatories were tied to organizations linked to or funded by Big Tech.[422]

However, there are also promising signals that this narrative is not being internalized wholesale within the US government. In a bold pro-competition statement in July 2021, the Biden administration's Executive Order on Competition took direct aim at the logic of this kind of anti-competition lobbying, declaring that "the answer to the rising power of foreign monopolies and cartels is not the tolerance of domestic monopolization, but rather the promotion of competition and innovation by firms small and large, at home and worldwide."[423]

Meanwhile, and rather awkwardly for those using the argument that China's threat should preclude pro-competition regulation in the US, the Chinese government has made several public moves toward tougher antitrust enforcement of its own national champions such as Alibaba and Tencent.[424] Some argue this signals the Chinese state reasserting control over private industry, by using the threat of competition enforcement to nudge the companies to align their business strategies with the government's industrial policy.[425] FTC chair Lina Khan, when asked to make sense of China's growing and aggressive stance toward its own Big Tech players, tacitly gestured to this analysis: "There's been a

[417] ACCESS Act of 2021, H.R. 3849, 117th Congress (2021–2022), https://www.congress.gov/bill/117th-congress/house-bill/3849/text.
[418] Platform Competition and Opportunity Act of 2021, H.R. 3826, 117th Congress (2021–2022), https://www.congress.gov/bill/117th-congress/house-bill/3826/text.
[419] Ending Platform Monopolies Act, H.R. 3825, 117th Congress (2021–2022), https://www.congress.gov/bill/117th-congress/house-bill/3825/text.
[420] Computer & Communications Industry Association, "National Security Issues Posed by House Antitrust Bills."
[421] Zachary Basu and Margaret Harding McGill, "Ex-intel officials claim antitrust could hurt U.S. in China tech race," Axios, September 15, 2021, https://www.axios.com/2021/09/15/china-antitrust-big-tech-national-security.
[422] Emily Birnbaum, "Group Backed by Tech Giants Claims Thousands of Members. Many Have Never Heard of It," *Politico*, March 30, 2022, https://www.politico.com/news/2021/09/22/former-security-officials-antitrust-tech-ties-513657.
[423] White House, "Executive Order on Promoting Competition in the American Economy."
[424] See Jana Kasperkevic, "Chinese Antitrust 2.0: Why Is China Going After Its Big Tech?" ProMarket, April 9, 2021, https://www.promarket.org/2021/04/09/chinese-antitrust-exceptionalism-enforcement-trade-alibaba-zhang; and "Alibaba And Tencent Fined In China Tech Crackdown," *Forbes*, July 13, 2022, https://www.forbes.com/sites/qai/2022/07/13/alibaba-and-tencent-fined-in-china-tech-crackdown.
[425] See Angela Huyue Zhang, "What Does Beijing Achieve from Regulating Its Big Tech?" U.S.-Asia Law Institute (USALI), April 20, 2021, https://usali.org/usali-perspectives-blog/what-does-beijing-achieve-from-regulating-its-big-tech; and see generally Angela Huyue Zhang, *Chinese Antitrust Exceptionalism* (Oxford: Oxford University Press, 2021).

recognition across jurisdictions that if you allow unfettered monopoly power to concentrate, its power can rival that of the state."[426]

## Loosely backed claims around Chinese approaches to privacy regulation are being used to advocate for a race to the bottom.

In the sphere of data privacy and AI accountability, similar to the conversation around antitrust, the US-China "AI race" is wielded as a lever advocating against further regulation. In this case, any restrictions or added friction proposed in how companies utilize the data of its users is contrasted against the notion that Chinese companies operate with unfettered access to citizen's data, and that the Chinese state exclusively supports rather than hinders this access.[427] Mark Zuckerberg noted that consent requirements for facial recognition create the risk of "falling behind Chinese competitors."[428] More recently, the vice president of the US Chamber of Commerce argued that the proposed federal privacy bill, American Data Privacy and Protection Act, intended to bring the US in line with the EU and a growing number of countries with data privacy laws, could hinder the competitiveness of US companies at a time when "the US is in a global race with China to lead the world in AI."[429] While the Chinese government's record of surveillance and intrusion into its citizens' lives is well documented, these claims that frame China as a regulatory vacuum are contradicted by the growing body of data security and data protection regulation in China.[430] While these analysts neither endorse Chinese privacy regulation as sufficient nor equate these laws with guaranteeing meaningful enforcement, they do dispel any lazy assertions that Chinese companies have unregulated access to the personal data they are permitted to collect and use.[431] They also draw more attention to the US as a global outlier when it comes to the lack of federal privacy protections.[432]

[426] "CNBC Transcript: Federal Trade Commission Chair Lina Khan Speaks Exclusively with Andrew Ross Sorkin and Kara Swisher Live from Washington, D.C. Today," CNBC, January 19, 2022, https://www.cnbc.com/2022/01/19/cnbc-transcript-federal-trade-commission-chair-lina-khan-speaks-exclusively-with-andrew-ross-sorkin-and-kara-swisher-live-from-washington-dc-today.html.

[427] See Graham Webster and Scarlet Kim, "The Data Arms Race Is No Excuse for Abandoning Privacy," Foreign Policy, August 14, 2018, https://foreignpolicy.com/2018/08/14/the-data-arms-race-is-no-excuse-for-abandoning-privacy; and "AI Arms Race: China and the Confucian-Communist Edge," Eye on AI, March 8, 2019, https://www.eye-on.ai/ai-articles/2019/3/8/ai-arms-race-china-and-the-confucian-communist-edge.

[428] Natasha Lomas, "Zuckerberg Urges Privacy Carve Outs to Compete with China," TechCrunch, April 10, 2018, https://techcrunch.com/2018/04/10/zuckerberg-urges-privacy-carve-outs-to-compete-with-china.

[429] Jordan Crenshaw, "What Should and Should Not Be Included in a National Privacy Bill," U.S. Chamber of Commerce, September 13, 2022, https://www.uschamber.com/technology/data-privacy/what-should-and-should-not-be-included-in-a-national-privacy-bill.

[430] See Rogier Creemers, "China's Emerging Data Protection Framework," *Journal of Cybersecurity* 8, no. 1 (2022), https://academic.oup.com/cybersecurity/article/8/1/tyac011/6674794; Amba Kak and Samm Sacks, "Shifting Narratives and Emergent Trends in Data-Governance Policy: Developments in China, India, and the EU," policy memo, Yale Law School, Paul Tsai China Center, August 2021, https://law.yale.edu/sites/default/files/area/center/china/document/shifting_narratives.pdf; Samm Sacks, Qiheng Chen, and Graham Webster, "Five Important Takeaways From China's Draft Data Security Law," New America, July 9, 2020, https://www.newamerica.org/cybersecurity-initiative/digichina/blog/five-important-take-aways-chinas-draft-data-security-law; Graham Webster, "Chinese Experts Push Data Privacy as Epidemic Systems Proliferate," New America, March 2, 2020, https://www.newamerica.org/cybersecurity-initiative/digichina/blog/chinese-experts-push-data-privacy-epidemic-systems-proliferate; and Graham Webster and Rogier Creemers, "A Chinese Scholar Outlines Stakes for New 'Personal Information' and 'Data Security' Laws (Translation)," New America, May 28, 2020, https://www.newamerica.org/cybersecurity-initiative/digichina/blog/chinese-scholar-outlines-stakes-new-personal-information-and-data-security-laws-translation.

[431] Samm Sacks and Lorand Laskai, "China's Privacy Conundrum," *Slate*, February 7, 2019, https://slate.com/technology/2019/02/china-consumer-data-protection-privacy-surveillance.html.

[432] Ralph Jennings, "What the US Might Learn From China's Data Privacy Rules," Voice of America (VOA), March 28, 2022, https://www.voanews.com/a/what-the-us-might-learn-from-china-s-data-privacy-rules-/6505203.html. For example, the US government's proposed ban on Chinese social media company TikTok, based on potential theft or misuse of American's data, has prompted many to point out that a federal privacy law, much more than an app ban, would go further to protect and mitigate the abuse of personal data in the US. See Glenn S. Gerstell, "The Problem with Taking TikTok Away from Americans," *New York Times*, February 1, 2023, https://www.nytimes.com/2023/02/01/opinion/tiktok-ban-china.html; and Evan Greer (@evan_greer), "Let's say the Chinese government was using TikTok to surveil Americans. If you ban TikTok, the Chinese gov can just legally purchase the same info from data brokers, because the US has almost no privacy laws. Don't ban TikTok, pass a damn privacy law," Twitter, February 1, 2023, 6:42 p.m., https://twitter.com/evan_greer/status/1620930744725143552.

The other loosely backed argument in policy circles is that Chinese tech companies benefit from the claim that Chinese society doesn't care as much about privacy.[433] Kai-Fu Lee (a venture capitalist and former Big Tech engineer), for example, notes that "Chinese users tend to be more willing to trade some degree of privacy for security or convenience."[434] Indeed, policy experts point out that US legislative proposals to counter Chinese data collection do not address the enormous amounts of user data collected and monetized by the likes of US-based Google, Apple, Facebook, and Amazon.[435] This assertion, too, is contradicted by the growing consumer and worker activism in China that resists technology-related concerns, such as the hotly debated issue of the use of facial recognition in public spaces and residential areas.[436]

We're starting to see similar anti-regulation arguments emerge in the context of algorithmic or AI accountability frameworks. The SCSP (the privately funded lobbying organization run by former tech industry executives and national security officials), for example, distances the US from the EU, which is debating legislation intended to regulate AI technologies. Instead, one argument goes, the US should aim for "non-regulatory approaches to governance" for AI, without clearly defining what those approaches are or how they might work in practice.[437]

---

### Increasing bipartisan consensus favors greater government intervention for developing AI as a strategic technology to ensure future prosperity.

**While policy initiatives often pitch this as a means to "democratize" and deconsolidate the AI industry, without a deliberate effort, this claim is on shaky ground. Current industrial policy proposals claim to "democratize AI," but risk being ultimately structured to in ways that entrench Big Tech firms' advantage and power.**

The "AI race" with China has perhaps been the single most productive argument behind the proliferation of policy instruments that increase government support and funding for the development of AI and other ancillary strategic technologies like semiconductors.[438] While the phrase "industrial policy" has historically been an uncomfortable and polarizing term in US politics given its associations with centrally directed economies (the SCSP has called it a "fraught label"), it is receiving increasing bipartisan support—a reflection of a growing trend in US politics to associate the national interest with the promotion of certain sectors of the economy.[439]

[433] See "AI Arms Race: China and the Confucian-Communist Edge"; and Qian Zhecheng, "Chinese Consumers Most Willing to Trade Privacy for Convenience," Sixth Tone, June 15, 2018, https://www.sixthtone.com/news/1002467/chinese-consumers-most-willing-to-trade-privacy-for-convenience.

[434] Lee also argues that "views about privacy are deeply embedded culturally. In China, there's pretty strong enforcement of laws against those who sell users' private data. The punishments are probably stronger even than in the U.S. or Europe. At the same time, Chinese users tend to be more willing to trade some degree of privacy for security or convenience." See Peter Schwartz, "Dr. Kai-Fu Lee on Why AI Redefines What It Means to Be Human," Salesforce, September 7, 2018, https://www.salesforce.com/content/blogs/us/en/2018/09/kai-fu-lee-ai-redefines-human-machine.html.

[435] See Alexandra S. Levine, "A U.S. Privacy Law Seemed Possible This Congress. Now, Prospects Are Fading Fast," *Politico*, June 1, 2022, https://www.politico.com/news/2021/06/01/washington-plan-protect-american-data-silicon-valley-491405; and Danny Crichton, "GDPR, China and Data Sovereignty Are Ultimately Wins for Amazon and Google," TechCrunch, May 29, 2018, https://techcrunch.com/2018/05/29/gdpr-and-the-cloud-winners.

[436] See Lakshmi Iyengar, "Major Chinese City Pushes Back Against Widespread Facial Recognition," Radii, October 30, 2020, https://radii.co/article/hangzhou-facial-recognition; and Whittaker, Ahmed, and Kak, "China in Global Tech Discourse."

[437] Special Competitive Studies Project, "Mid-Decade Challenges to National Competitiveness." See page 35.

[438] Joel Mathis, "The CHIPS Act and Industrial Policy, Explained," *The Week*, August 2, 2022, https://theweek.com/economy/1015566/the-chips-act-and-industrial-policy-explained.

[439] See David Leonhardt, "An Investment With a Big Return," *New York Times*, June 8, 2021, https://www.nytimes.com/2021/06/08/briefing/investment-senate-china-bill.html; Scott Lincicome, "Conservative Industrial Policy and the 'China Threat'," Cato Institute (blog), August 28, 2020, https://www.cato.org/blog/conservative-industrial-policy-china-threat; Scott Lincicome and Huan Zhu, "Questioning Industrial Policy: Why Government Manufacturing Plans Are Ineffective and Unnecessary," Cato Institute, 2021, https://www.cato.org/sites/cato.org/files/2021-09/white-paper-questioning-industrial-policy-updated.pdf; and David E. Sanger, Catie Edmondson,

Notably, this argument in favor of greater government support to develop the AI industry originally took shape in the form of a critique of private-sector consolidation in the tech industry. The NSCAI was forthcoming in its 2022 final report that the consolidation of the AI industry is a "threat" to US competitiveness, with a detailed analysis of how the "brain drain" from other sectors of the economy (from small AI startups to local, state, and federal government) to a few big Silicon Valley tech firms, alongside the astronomical compute costs required to train large-scale AI models means that "AI startups have narrowing paths to growth in the United States."[440] They even argue that a highly concentrated tech industry is contributing to the lack of diversity in the AI field, which limits the ability to "build equitable, inclusive systems."[441] This is a problem, the argument goes, because commercial priorities are driving the technology agenda rather than an organized public-private effort, and so the eventual recommendations are to "blend" public and private resources into these strategic technology domains.

This concern with consolidation in private industry, however, has remained superficial in policy proposals that have followed from other organizations in the space. The National AI Research Resource (NAIRR), an initiative designed by the National Science Foundation and the White House Office of Science and Technology Policy, cites the NSCAI's report while proposing a kind of AI data and compute infrastructure commons that researchers around the country can access, with the aim of "democratizing AI'' and addressing consolidation.[442] However, as we pointed out in an official submission to the NAIRR task force, the NAIRR project as it is currently envisioned falls back on "leveraging public-private partnerships'' to provide this resource rather than the government creating these compute resources themselves, building an alternative to Big Tech infrastructure.[443] This reinforces that the only plausible short- to mid-term scenario is that the infrastructure required for NAIRR would be licensed from the very same Big Tech companies that currently control them. The director of the Stanford Institute for Human-Centered Artificial Intelligence (HAI), which credits itself with first conceptualizing the NAIRR project, makes these dependencies explicit, arguing that "the commercial cloud providers are already doing the innovation, and they invest massive amounts of money to keep it up-to-date," and that therefore there is no need for the government to create these resources themselves.[444] The NSCAI and SCSP's recommendations have also paved the way for a slew of legislation that explicitly focuses on bolstering government R&D spending toward American tech development (including subsidies for manufacturing) with no discernible focus on reducing the dependencies on Big Tech data or compute infrastructures.[445]

David McCabe, and Thomas Kaplan, "Senate Poised to Pass Huge Industrial Policy Bill to Counter China," *New York Times*, June 7, 2021, https://www.nytimes.com/2021/06/07/us/politics/senate-china-semiconductors.html.

[440] National Security Commission on Artificial Intelligence, *Final Report*. See page 187.

[441] Ibid.

[442] See Amba Kak, Brittany Smith, Sarah Myers West, and Meredith Whittaker, "Request for Information (RFI) on an Implementation Plan for a National Artificial Intelligence Research Resource," AI Now Institute and Data and Society, October 1, 2021, https://ainowinstitute.org/AINow-DS-NAIRR-comment.pdf; and NAIRR Task Force, "Envisioning a National Artificial Intelligence Research Resource (NAIRR): Preliminary Findings and Recommendations, NAIRR-TF-Interim-Report-2022.pdf.

[443] Kak, Smith, West, and Whittaker, "Request for Information (RFI) on an Implementation Plan for a National Artificial Intelligence Research Resource."

[444] See Jeffrey Mervis, "U.S. Law Sets Stage for Boost to Artificial Intelligence Research," Stanford Human-Centered Artificial Intelligence, January 19, 2021, https://hai.stanford.edu/news/us-law-sets-stage-boost-artificial-intelligence-research; John Etchemendy and Fei-Fei Li, "National Research Cloud: Ensuring the Continuation of American Innovation," Stanford Human-Centered Artificial Intelligence, March 28, 2020, https://hai.stanford.edu/news/national-research-cloud-ensuring-continuation-american-innovation; and John Thornhill, "A Public Research Cloud Would Stimulate Innovation," *Financial Times*, October 18, 2020 https://www.ft.com/content/b5928d21-602e-4f10-bdf6-f0c123a96bfe.

[445] See United States Innovation and Competition Act of 2021, S. 1260, 117th Congress (2021–2022), https://www.congress.gov/bill/117th-congress/senate-bill/1260 (passed Senate); United States Innovation and Competition Act of 2021, H.R. 4521, 117th Congress (2021–2022), https://www.congress.gov/bill/117th-congress/house-bill/45212021 (passed Senate); and Advancing American AI Act, S. 1353, 117th Congress (2021–2022), https://www.congress.gov/bill/117th-congress/senate-bill/1353/text (reported to Senate).

The inherent contradictions abound, though they are rarely broken down in any detail. On the one hand, rhetorical moves that draw on the "arms race" narrative position the "command and control" Chinese economy with its often-caricatured lack of state-private divide in contrast to the freedom of private enterprise in the Western liberal political economy (this is a key justification for the recent restrictions on Americans investing in Chinese technology.)[446] But policy recommendations designed to address the arms race are designed around the development of US industrial policy in the sphere of AI and related strategic technologies, putting this differentiator on increasingly shaky ground. While the infusion of public investment has been loosely conflated with the "democratization" of AI, in practice the identification of AI as a strategic national asset would end up bolstering the advantage of the largest tech companies and eventually protect these companies from structural regulation. All of these movements are presently unfolding largely unchecked, and deserve close scrutiny.

[446] White House, "Executive Order on Addressing the Threat from Securities Investments That Finance Certain Companies of the People's Republic of China," June 3, 2021, https://www.whitehouse.gov/briefing-room/presidential-actions/2021/06/03/executive-order-on-addressing-the-threat-from-securities-investments-that-finance-certain-companies-of-the-peoples-republic-of-china.

# AI Arms Race Timeline

| Event | Date | Key Figures | Quote |
|---|---|---|---|
| **Eric Schmidt gives keynote address at global security summit emphasizing technological competition with China** | 13 November 2017 | Paul Scharre (Vice President and Director of Studies at CNAS), Eric Schmidt (ex Google CEO); Center for a New American Security (policy thinktank) | "By 2020 they will have caught up. By 2025 they will be better than us, and by 2030 they will dominate the industries of AI." |
| **National Security Commission on Artificial Intelligence established, chaired by ex-Google CEO Eric Schmidt** | 13 Aug 2018 | Eric Schmidt (ex Google CEO) | |
| **Facebook (Meta) CEO Mark Zuckerberg argues that privacy rights will make US tech fall behind Chinese competitors** | 14 Aug 2018 | Mark Zuckerberg (Meta CEO) | |
| **Kai-Fu Lee, author of AI superpowers and ex-head of Google China, highlights growing chill in US/China tech relations** | 26 September 2018 | Kai Fu Lee (author, ML engineer and venture capitalist, ex Microsoft, ex Google) | "I think cross-border will be very difficult," he said. "I wouldn't advise you to work for an American company trying to do business in China, or a Chinese company trying to do business in America — tech company anyway." |
| **President and CEO of the Atlantic Council argues that China is getting the upper hand in the AI arms race** | 26 Jan 2019 | Frederick Kempe (president and chief executive officer of the Atlantic Council) | "Though it is a tech race most Western executives feel is only on its first laps, they heard how President Xi had declared a sort of space race or Manhattan Project around AI that is already delivering measurable results." |
| **CEO of AI news platform Eye on AI claims that China's authoritarian, Confucian culture gives them an edge in the AI arms race** | 8 March 2019 | Craig Smith (former NYT journalist, CEO of Eye on AI, NSCAI podcast host) | "China is awash in data like no other country and with the Communist Party on one side and Confucian culture on the other, that data is being used to train AI systems with little of the resistance met in the West." |
| **Sheryl Sandberg, Eric Schmidt and other Big Tech leaders argue that antitrust law will decrease US competitiveness with China** | 23 May 2019 | Sheryl Sandberg (ex COO Facebook); Eric Schmidt (ex Google CEO) | Sandberg: "While people are concerned with the size and power of tech companies, there's also a concern in the United States with the size and power of Chinese companies, and the realization that these companies are not going to be broken up." |

| Event | Date | Key Figures | Quote |
|---|---|---|---|
| **Henry Kissinger, Eric Schmidt and an MIT computer professor publish a book about the 'Age of AI' and the importance of Big Tech** | January 2021 | Henry A. Kissinger, Eric Schmidt, Daniel Huttenlocher | The book brings together Henry Kissinger, an eminent computer scientist and ex-Google CEO Eric Schmidt to consider the advent of a so-called "age of AI". |
| **The National Security Commission on AI Releases its Final Report, Claims that China's AI development is a threat to all Americans** | May 2021 | Eric Schmidt (ex-Google CEO) | "The United States must act now to field AI systems and invest substantially more resources in AI innovation to protect its security, promote its prosperity, and safeguard the future of democracy." |
| **Two US Senators send letter to National Science Foundation urging that AI is developed in line with 'American Values'** | 13 May 2021 | Martin Heinrich (D-N.M.); Rob Portman (R-Ohio), | “AI leadership by the United States is only possible if AI research, innovation, and use is rooted in American values." |
| **Executive Order on Addressing the Threat from Securities Investments that Finance Certain Companies of the People’s Republic of China** | 3 June 2021 | President Joseph Biden | "the administration’s emphasis on China’s “military-industrial complex” (and “Chinese military-industrial complex companies”) could send the wrong message" |
| **Biden Administration Releases Executive Order on Competition to promote US Domestic Innovation against 'Foreign Cartels'** | July 2021 | President Joseph Biden | "This order reasserts as United States policy that the answer to the rising power of foreign monopolies and cartels is not the tolerance of domestic monopolization, but rather the promotion of competition and innovation by firms small and large, at home and worldwide" |
| **Leading tech advocacy organization publishes white paper critiquing antitrust bills as threat to US national security interests and the 'innovation race' with China** | September 2021 | Computer and Communications Industry Association | "The House of Representatives is considering several bills targeting leading U.S. technology firms with sweeping provisions that are in serious tension with the overall U.S. national innovation strategy to combat China and other adversaries." |
| **12 former security officials publish letter arguing that US antitrust law undermines the US tech innovation system and makes China more competitive with the US** | 15 September 2021 | Robert Cardillo, Dan Coats, Admiral James Foggo III, Richard H. Ledgett Jr., John D. Negroponte, Leon E. Panetta, Vice Admiral Jan E. Tighe, Frances Townsend, Susan M. Gordon, Michael Morell, Dr. Michael Vickers, Admiral James “Sandy” Winnefeld Jr. | "We strongly believe it is in the best interest of our national and economic security to prevent China from achieving its objective of becoming the global leader in technological innovation." |

| Event | Date | Key Figures | Quote |
|---|---|---|---|
| **12 former security officials who warned against US antitrust law revealed to have ties to Big Tech** | 22 September 2021 | Leon Panetta (ex Secretary of Defense); Dan Coats (ex Director of National Intelligence) | "The warning last week from a dozen former national security leaders was stark: An antitrust crackdown on Silicon Valley could threaten the nation's economy and "cede U.S. tech leadership to China." |
| **Special Competitive Studies Project founded to address intensifying geopolitical competition with China and Russia in the "age of AI".** | October 2021 | Eric Schmidt (ex-Google CEO); William McClellan "Mac" Thornberry (ex-Representative of Texas, Republican); Robert O. Work (ex Deputy Secretary of Defense); Nadia Schadlow (ex Deputy National Security Advisor for Strategy); Michèle Flournoy (ex Under Secretary of Defense for Policy) | "We want to ensure that America is positioned and organized to win the techno-economic competition between now and 2030, the critical window for shaping the future." "Technology competition has become a key element of a systemic competition over world over" |
| **Microsoft ends partnership with leading Chinese drone company DJI after it is sanctioned by the US Treasury** | December 2021 | | "It has also been rumored that Microsoft has stopped recruiting from some Chinese universities." |
| **MIT Tech Review investigation reveals that charges brought by the US Department of Justice's China Initiative have little to do with national security.** | 2 December 2021 | | "Instead of focusing on economic espionage and national security, the initiative now appears to be an umbrella term for cases with almost any connection to China" |
| **White House names AI on its Critical and Emerging Technologies list of tech that could inform national security activities** | February 2022 | National Science and Technology Council | Congress establishes the National Security Commission on Artificial Intelligence, chaired by ex-Google CEO Eric Schmidt |
| **Senate passes the United States Innovation and Competition Act to combat Chinese tech growth, at the expense of regulating US Big Tech** | June 2022 | Jan Schakowsky (D-Ill.) | "A top House Democrat and advocacy groups are sounding the alarm over a trade provision in legislation to bolster US competitiveness they say would obstruct regulation of large technology companies." |
| **The Pentagon's new digital and AI chief asks Eric Schmidt for help solving the DOD's software problem** | 7 June 2022 | Craig Martell (ex Lyft and the Pentagon's first permanent chief digital and artificial intelligence officer (CDAO)); Eric Schmidt (ex Google | "He's [Schmidt] one of many top technology players to raise concerns recently about the DOD's ability to improve its software capabilities to effectively compete with global powers like China." |

| Event | Date | Key Figures | Quote |
|---|---|---|---|
| **Senator Rand Paul argues that protecting the US free market for Big Tech is essential for competing with China** | 13 June 2022 | Rand Paul (Republican Senator, Kentucky) | "Politicians who are fretting about China's drive for global economic dominance should think twice before dismantling the U.S. firms that invest heavily in artificial intelligence and can compete worldwide."" |
| **Eric Schmidt and Harvard professor argue that Biden needs to launch a huge tech recruitment program to compete with China** | 16 July 2022 | Graham Allison, a professor of government at the Harvard Kennedy School, and Eric Schmidt | "Immigration is the United States' secret sauce—including in its competition with China." |
| **Bipartisan CHIPS act is passed, blocking certain chip exports to China, reducing its ability to make semiconductors** | 9 August 2022 | Biden administration | "The Act also includes safeguards to ensure that recipients of Federal funds from these programs cannot build advanced semiconductor production facilities in countries that present a national security concern." |
| **Succeeding in the AI Competition with China: A Strategy for Action** | September 2022 | Brookings | "Technology is at the center of the emerging competition between the United States and China, with far-reaching consequences for democratic societies." |
| **Two US senators send the director of national intelligence a letter of concern regarding a proposed partnership between Apple and Chinese chipmaker Yangtze Memory Technologies Co** | September 2022 | Mark Warner (Democratic chair of Senate intelligence committee); Marco Rubio (Republican Vice Chair) | "Such a decision would introduce significant privacy and security vulnerabilities to the global digital supply chain that Apple helps shape given YMTC's extensive, but often opaque, ties to the Chinese Communist party." |
| **Special Competitive Studies Project releases first report framing US-China competition as the "defining feature of world politics today"** | 24 September 2022 | Eric Schmidt (ex-Google CEO); William McClellan "Mac" Thornberry (ex-Representative of Texas, Republican); Robert O. Work (ex Deputy Secretary of Defense); Nadia Schadlow (ex Deputy National Security Advisor for Strategy); Michèle Flournoy (ex Under Secretary of Defense for Policy) | "The epicenter of the competition is the quest for leadership and dominant market share in a constellation of emerging technologies that will underpin a thriving society, growing economy, and sharper instruments of power." |

| Event | Date | Key Figures | Quote |
|---|---|---|---|
| **US Chamber of Commerce VP Jordan Crenshaw flags AI arms race at House Subcommittee on Trustworthy AI** | 29 September 2022 | Jordan Crenshaw (VP Chamber of Commerce) | "When it comes to AI, we're in a race we must win...We cannot afford to sit on the sidelines and allows those who do not share our democratic values set the standard for the world" |
| **Advancing American AI Act directly cites recommendations from the NSCAI and emphasizes restricting Chinese tech** | 29 September 2022 | Rob Portman (Republican Senator, Ohio); Gary Peters (Democrat Senator, Michigan); Eric Schmidt (ex Google) | The director is to consider "the considerations and recommended practices identified by the National Security Commission on Artificial Intelligence in the report entitled “Key Considerations for the Responsible Development and Fielding of AI’" |
| **Advancing American AI Act submitted as amendment to the defense budget, alongside other amendments aiming to restrict Chinese tech development** | 21 October 2022 | Rob Portman (Republican Senator, Ohio); Gary Peters (Democrat Senator, Michigan) | "Another amendment seeks to share technology and other military equipment with Taiwan to further the U.S.’s economic partnership with the island, while the Israel-U.S. AI partnership would prohibit working with any entity that is linked to China." |
| **Brief about Emerging Non-European Monopolies in the Global AI Market highlights US' and China's lead** | November 2022 | Future of Life Institute (Oxford) | Argues that all of the cutting-edge general purpose AI models have been developed outside of the EU, with a focus on US and Chinese institutions. |
| **U.S. expands bans of Chinese security cameras and network equipment, citing national security threat** | November 2022 | Federal Communications Commission (FCC) | "The Federal Communications Commission voted 4-0 to ban sales of new telecom and surveillance equipment made by several Chinese companies, arguing that their ownership and practices threaten U.S. national security." |
| **President of the Information Tech and Innovation Foundation critiques antitrust law as threat to national competitiveness** | 4 November 2022 | Robert Atkinson, president of the Information Technology and Innovation Foundation | "They don’t think about the implications of their actions on US competitiveness. Their only goal is to think about whether it is going to lead to more competition” |
| **Former Trade Policy Counsel argues that antitrust crackdowns on Big Tech will hurt the US in competition with China** | 9 November 2022 | Clark Packard (Former Trade Policy Counsel, Finance Insurance & Trade) | "Today, Beijing is trying to supplant the United States as the global leader for the commanding heights of technology. Healthy competition should be welcomed, but Beijing’s methods are unsavory." |

| Event | Date | Key Figures | Quote |
|---|---|---|---|
| **Fortune frames chatGPT as part of the AI arms race between the US and China** | January 2023 | Fortune | "ChatGPT is a salvo in a growing generative A.I. 'arms race' between the U.S. and China" |
| **FBI director argues China's AI program will be weaponized against the US at Davos** | 20 January 2023 | Christopher Wray (FBI Director) | "The Chinese government has a bigger hacking programme than any other nation in the world." |
| **US Chamber of Commerce Report on AI Explicitly Cites Threat of China's Rise As Driving Factor Behind US AI Innovation Plans, Promotes Private-Military US Partnerships in Response** | March 2023 | US Chamber of Commerce Commission on Artificial Intelligence Competitiveness, Inclusion, and Innovation | "To capitalize on American ingenuity, Congress and the Pentagon must look at streamlining acquisition processes and finding new ways of incorporating industry expertise and experience within the military enterprise" |

Spotlight

# The Climate Costs of Big Tech

**Big-Tech infrastructures are locking us into an unsustainable future. The climate costs wrought by Big Tech intersect with and build upon the harms of other unjust systems, structures, and processes, including the racism of capitalism and settler colonialism.**

The constant push for scale in artificial intelligence has led Big Tech firms to develop hugely energy-intensive computational models that optimize for “accuracy” - through increasingly large datasets and computationally intensive model training - over more efficient and sustainable alternatives.[447] As we increasingly become locked into using Big-Tech infrastructures, we also become locked into their voracious appetite for resources: data centers have high energy costs and carry a massive carbon footprint.[448] Computing technologies rely heavily on minerals that are procured under violent and exploitative conditions.[449] But these environmental harms are not evenly distributed; they disproportionately impact communities that are already marginalized, in a manner that reenacts historical practices of settler colonialism and racial capitalism.[450]

[447] See Roy Schwartz, Jesse Dodge, Noah A. Smith, and Oren Etzioni, “Green AI,” arXiv:1907.10597v3, August 13, 2019, https://arxiv.org/abs/1907.10597; and Becky Kazansky, Madhuri Karak, Teresa Perosa, Quito Tsui, and Sara Baker, “At the Confluence of Digital Rights and Climate & Environmental Justice: A Landscape Review,” Engine Room, 2022, https://www.theengineroom.org/wp-content/uploads/2022/07/TER-Executive-Sumary04-07-22.pdf.

[448] Emma Strubell, Ananya Ganesh, and Andrew McCallum, “Energy and Policy Considerations for Deep Learning in NLP,” arXiv: 1906.02243v1, June 5, 2019, https://arxiv.org/abs/1906.02243.

[449] Michael Kwet, “A Digital Tech Deal: Digital Socialism, Decolonization, and Reparations for a Sustainable Global Economy,” Global Information Society Watch, August 10, 2020, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3670986.

[450] See Max Liboiron, *Pollution Is Colonialism* (Durham, NC: Duke University Press, 2021); and Emily Bender, Timnit Gebru, Angelina McMillan-Major, Shmargaret Shmitchell, “On the Dangers of Stochastic Parrots: Can Language Models Be Too Big?” *FAccT ‘21: Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency*, March 2021, https://dl.acm.org/doi/10.1145/3442188.3445922.

**While the carbon costs of data centers have been the primary focus of attention in the news, data centers also rely on immense amounts of water for both electricity production and cooling.[451] To supply their centers, many tech firms draw from public water supplies and aquifers, adding to regional water stress—while being built in some of the world's most drought-prone areas.**

To cool down servers and prevent overheating, data centers require immense amounts of water for electricity generation.[452] Companies often draw on public water supplies that are already strained after decades of growth and underinvestment in public infrastructure,[453] though the amount drawn from existing supplies is difficult to verify because many companies' water use is largely non-transparent (some companies publish limited figures).[454] Despite this heavy reliance on water, data centers are being built in areas already experiencing high levels of regional water stress (including the West and Southwest US)[455], leading community and conservation groups all over the world to protest the construction of new data centers in their neighborhoods.[456] Pushback has been moderately successful—for example, following extensive controversy over the impact of data centers on local residents' water supply and the likelihood that certain provinces were facing seasonal water shortages, organizers pushed the Netherlands to temporarily ban the new construction of data centers.[457]

---

**Big Tech firms are setting out ambitious public sustainability goals, but are failing to follow through.**

Driven by worker-led activism and negative headlines about tech's climate costs, large technology firms have been vocally supportive of climate action and have announced ambitious public sustainability goals. But these amount to little more than a marketing ploy.

Several tech firms have made significant sustainability pledges, including Microsoft's promise to be carbon negative by 2030[458] and to reduce data-center water usage by 94 percent by 2024,[459] and

[451] April Anson, Andrea Ballestero, Dean Chahim, CIEJ, Theodora Dryer, Sage Gerson, Matthew Henry, Hi'ilei Julia Hobart, Fushcia-Ann Hoover, J.T. Roane, Amrah Salomón, Bruno Seraphin, and Elena Sobrino, "Water Justice and Technology: The COVID-19 Crisis, Computational Resource Control, and Water Relief Policy," AI Now Institute, January 10, 2022, https://ainowinstitute.org/water-justice-technology.html.

[452] See David Mytton, "Data Centre Water Consumption," *npj Clean Water* 4, no. 11 (2021), https://www.nature.com/articles/s41545-021-00101-w; Farhana Sultana, "The Unbearable Heaviness of Climate Coloniality," *Political Geography* 99 (November 2022), https://www.sciencedirect.com/science/article/abs/pii/S096262982200052X; Masaō Ashtine and David Mytton, "We Are Ignoring the True Cost of Water-Guzzling Data Centres," *Conversation*, October 19, 2021, https://theconversation.com/we-are-ignoring-the-true-cost-of-water-guzzling-data-centres-167750; and Caroline Donnelly, "Why Water Usage Is the Datacentre Industry's Dirty Little Secret," *Computer Weekly*, September 21, 2021, https://www.computerweekly.com/blog/Ahead-in-the-Clouds/Why-water-usage-is-the-datacentre-industrys-dirty-little-secret.

[453] Nikitha Sattiraju, "Google Data Centers' Secret Cost: Billions of Gallons of Water," Bloomberg, April 1, 2020, https://www.bloomberg.com/news/features/2020-04-01/how-much-water-do-google-data-centers-use-billions-of-gallons.

[454] Microsoft and Facebook currently publish aggregated water data. See "Reports Hub," Corporate Social Responsibility, Microsoft, accessed March 3, 2023, https://www.microsoft.com/en-us/corporate-responsibility/reports-hub; and "Water," Sustainability, Meta, accessed March 14, 2023, https://sustainability.fb.com/water.

[455] Gauthier Roussilhe, "The Hidden Costs of Data Centers," July 21, 2022, in World Wide Waste with Gerry McGovern, This Is HCD, podcast, MP3 audio, 50:00, https://www.thisishcd.com/episode/gauthier-roussilhe-the-hidden-costs-of-data-centers.

[456] See Olivia Solon, "Drought-Stricken Communities Push Back against Data Centers," NBC News, June 19, 2021, https://www.nbcnews.com/tech/internet/drought-stricken-communities-push-back-against-data-centers-n1271344; and Bo Petersen, "Google's Controversial Groundwater Withdrawal Sparks Question of Who Owns South Carolina Water," *Post and Courier*, April 22, 2017, https://www.postandcourier.com/news/google-s-controversial-groundwater-withdrawal-sparks-question-of-who-owns/article_bed9179c-1baa-11e7-983e-03d6b33a01e7.html.

[457] Dan Swinhoe, "Update: Hollands Kroon Facing Drinking Water Shortage If New Data Centers Are Built," Data Center Dynamics (DCD), March 22, 2021, https://www.datacenterdynamics.com/en/news/hollands-kroon-facing-drinking-water-shortage-if-new-data-centers-are-built.

[458] Brad Smith, "Microsoft Will Be Carbon Negative by 2030," Microsoft (blog), January 16, 2020, https://blogs.microsoft.com/blog/2020/01/16/microsoft-will-be-carbon-negative-by-2030.

[459] Harry Menear, "Microsoft to Reduce Data Centre Water Usage by 94% by 2024," DataCentre, October 28, 2021, https://datacentremagazine.com/critical-environments/microsoft-reduce-data-centre-water-usage-94-2024.

Google's aim to shift its data centers to carbon-free electricity by 2030.[460] Many of these initiatives are reactive, designed in response to worker-led organizing: a day before a planned protest by Amazon Employees for Climate Justice, Jeff Bezos attempted to head the news cycle off at the pass by announcing a plan for Amazon to achieve net-zero emissions by 2040, and to match 100 percent of its power with renewable purchases by 2025.[461] But green nonprofits underscore that these initiatives are little more than marketing: one report by the New Climate Institute gave Amazon and Google's climate pledges a "low integrity" rating and Apple a "moderate integrity" rating, meaning that their accounting for emissions is inherently flawed or that they will fail to meet even their own modest targets.[462]

In fact, in some cases the emissions of many of the firms that have made such pledges actually grew: Microsoft's emissions increased from 11.6m metric tons of CO2 in 2020 to 13m metric tons in 2021.[463] Instead of taking on the harder work of reducing their carbon demand, firms are pouring hundreds of millions of dollars into carbon-removal technology and carbon offsets, even as their emissions continue to grow.[464] Such measures don't have a good track record of effectively permanently removing carbon dioxide from the atmosphere and aren't a substitute for reducing emissions overall.[465]

[460] Catherine Clifford, "How Google Plans to Use 100% Carbon-Free Energy in Its Data Centers by 2030," CNBC, April 13, 2022, https://www.cnbc.com/2022/04/13/google-data-center-goal-100percent-green-energy-by-2030.html.
[461] Leslie Hook and Dave Lee, "How Tech Went Big on Green Energy," *Financial Times*, February 10, 2021, https://www.ft.com/content/0c69d4a4-2626-418d-813c-7337b8d5110d.
[462] New Climate Institute, "Major Companies Largely Fail Net Zero Climate Pledge Test," press release, February 7, 2022, https://newclimate.org/news/press-release-corporate-climate-responsibility-monitor-2022.
[463] Microsoft, *2021 Environmental Sustainability Report: From Pledges to Progress*, 2021, https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4RwfV.
[464] Justine Calma, "Stripe, Alphabet, Meta, Shopify, and McKinsey Launch New Carbon Removal Initiative," *Verge*, April 12, 2022, https://www.theverge.com/2022/4/12/23022343/stripe-alphabet-meta-shopify-mckinsey-launch-carbon-removal-initiative-frontier.
[465] Justine Calma, "Big Tech Is Pouring Millions into the Wrong Climate Solution at Davos," May 25, 2022, *Verge*, https://www.theverge.com/2022/5/25/23141166/big-tech-funding-wrong-climate-change-solution-davos-carbon-removal.

## Greenwashing Timeline

| Date | Event | Actors |
|---|---|---|
| September 2019 | Amazon pledges to follow Paris Agreement and be carbon neutral by 2040 | Amazon |
| September 2019 | Employee walkout over sustainability/climate change | Microsoft, Google, Amazon |
| October 2019 | Guardian investigation finds that Google has been funding climate change deniers | Google, Guardian |
| September 2020 | Google announces that it will run on carbon free energy by 2030 | Google |
| September 2021 | Influence Map report finds that Big Tech's green rhetoric is not matched by policy action | Influence Map |
| February 2022 | New Climate finds that there is little integrity to Big Tech's climate goals | New Climate |
| April 2022 | Big Tech launches major initiative for carbon capture | Stripe, Alphabet, Meta, Shopify, and McKinsey |
| November 2022 | UN Panel Calls Out 'Greenwashers' and Seeks Net-Zero Regulation | UN expert group appointed by Secretary General António Guterres; chaired by Catherine McKenna |

### Despite their pledges, tech firms have either remained silent on or have actively opposed major climate policy initiatives.

Despite their strong rhetoric, tech firms are reticent to use their political capital in support of major climate policy initiatives. In the lead-up to the vote on the Inflation Reduction Act, which included the biggest climate investment in US history, tech companies largely stayed silent on their positions on the bill.[466] Another study found that only 6 percent of large tech firms' lobbying targets climate policy, suggesting a broad refusal to deploy their resources in support of environmentally friendly policy initiatives.[467]

In some instances, they are willing to make significant contributions to climate change deniers. For example, Google has made large contributions to the Competitive Enterprise Institute, a conservative group that influenced the Trump Administration to abandon the Paris Agreement.[468] The company also sponsored the annual meeting for the State Policy Network, an organization whose members created a "climate pledge" website asserting that "there is no climate crisis."[469]

[466] See Lisa Martine Jenkins, "Big Tech is largely silent on whether it supports the new climate bill," *Protocol*, July 29, 2022, https://www.protocol.com/climate/big-tech-ira-react; and Bill Weihl, "Where Was Big Tech on Historic Climate Legislation? (The Answer Might Surprise You)," GreenBiz, September 6, 2022, https://www.greenbiz.com/article/where-was-big-tech-historic-climate-legislation-answer-might-surprise-you.

[467] See InfluenceMap, *Big Tech and Climate Policy: An InfluenceMap Report*, January 2021, https://influencemap.org/report/Big-Tech-and-Climate-Policy-afb476c56f217ea0ab351d79096df04a; and Laura Paddison, "Big Tech's Pro-Climate Rhetoric Is Not Matched by Policy Action, Report Finds," *Guardian*, September 20, 2021,https://www.theguardian.com/environment/2021/sep/20/big-tech-climate-change.

[468] Lisa Friedman and Hiroko Tabuchi, "Following the Money That Undermines Climate Science," *New York Times*, July 10, 2019, https://www.nytimes.com/2019/07/10/climate/nyt-climate-newsletter-cei.html.

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